LANDesk® System Manager 8.7

Benutzerhandbuch



Inhalt

Übersicht

Informationen zu LANDesk® System Manager

Willkommen bei LANDesk® System Manager 8.70! Mit dieser unabhängigen Verwaltungsanwendung gewährleisten Sie, dass Ihre Server (einschließlich der Server, die Windows, Linux, HP-UX und AIX ausführen) verfügbar bleiben. Das Produkt kann auch zusammen mit LANDeskManagement Suite installiert und verwendet werden; dabei kann dieselbe Core-Datenbank wie Management Suite benutzt werden, um die IT-weite Berichterstattung zu ermöglichen.

Das vorliegende Produkt wurde unter dem Aspekt einer möglichst geringen Ressourcenbelastung entwickelt. Es verfügt über mehrere On-Demand-Agenten und -Dienste, die nur ausgeführt werden, wenn tatsächlich Bedarf besteht. Auf diese Weise werden Speicherressourcen und CPU-Zyklen für andere Tasks freigegeben. LANDesk weiß um die kritische Bedeutung der Ressourcenverfügbarkeit für Ihr Unternehmen. Aus diesem Grund stand bei der Entwicklung des Produkts die Stabilität und unterbrechungsfreie Ausführung in Rund-um-die-Uhr-Umgebungen im Vordergrund. Damit behalten Sie die Kontrolle über die auf Ihren Geräten ausgeführte Software. Sie können den vollständigen Agenten installieren, spezifische Komponenten auswählen oder Geräte in Ihre Geräteliste verschieben, ohne Agenten zu installieren.

Damit Dialogfelder und Fenster ordnungsgemäß angezeigt werden, muss die Website von System Manager der Liste mit den zulässigen Websites im Popup-Blocker des Browsers hinzugefügt werden.

Neue Funktionen in Version 8.70

Die folgenden Funktionen sind neu hinzugekommen oder wurden von der vorherigen Version von System Manager aktualisiert:

Geräteverwaltung ohne Agenten: Verwalten Sie Geräte in der Ansicht **Eigene Geräte**, ohne einen Verwaltungsagenten auf diesen Geräten zu installieren, wenn die Geräte mit einer Out-of-Band-Verwaltungstechnologie wie Intel* AMT, IPMI oder DRAC aktiviert sind.

Benutzerdefinierte Gruppen inGeplante Tasks: Sie können Tasks in benutzerdefinierten Gruppen zusammenfassen Ausführung zu ermöglichen.

Einsteigermodus: Sie können Bezeichnungen für die Schaltflächen auf den Symbolleisten anzeigen, damit neue Benutzer auf den ersten Blick erkennen, welche Aufgabe die jeweilige Schaltfläche erfüllt. Umgekehrt können Sie diese Bezeichnungen nach Bedarf ausblenden (die Kurzhilfe wird jedoch nach wie vor mit der Maus angezeigt).

Hardware-Konfiguration: Mit diesem neuen Tool können Sie Optionen für Geräte mit Intel* AMT-Funktionen erstellen. Sie können Kennungen (IDs) für die Versorgung von Intel AMT-Geräten generieren, die generierten IDs anzeigen und Konfigurationsoptionen für die Versorgung

Ihrer Intel AMT-Geräte ändern. Darüber hinaus können Sie Circuit Breaker-Richtlinien definieren und verdächtige Netzwerkaktivitäten auf Geräten blockieren.

Erweiterte Unterstützung für Active Management Technology. Ab diesem Release unterstützt das Produkt jetzt auch Intel* Active Management Technology 2 (zusätzlich zu Version 1). AMT Version 2 unterstützt zudem die Verwaltung ohne Agenten und automatische Erkennung von Intel* AMT 2-Geräten.

Produktfunktionen

Mit System Manager können Sie selbst über das angemessene Verwaltungsniveau für Ihre Umgebung entscheiden - von einfacher Informationserfassung bis hin zu komplexen Leistungsanalysen, Sicherheits- und Konfigurationskontrollen. System Manager umfasst Folgendes:

Einfach zu verwendende Webkonsole: Führen Sie das Produkt jederzeit und von überall aus mit einer webbasierten Konsole, die darauf ausgelegt ist, komplexe Daten in einer einfach zu bedienenden Benutzeroberfläche bereitzustellen. Sie können die Konsole von Ihrer primären Arbeitsstation oder von einer Arbeitsstation im Serverraum ausführen, ohne dass eine Installation durchgeführt werden muss. Navigieren Sie ganz einfach zur Produkt-URL, http://*coreserver*/LDSM. Wählen Sie bestimmte Geräte als "Ziel" zur Durchführung von Aktionen wie Softwareverteilungen aus, indem Sie sie zum Einfügen in die Liste **Zielgeräte** selektieren. Dieser Vorgang ähnelt dem Warenkorbmodell zahlreicher Webanwendungen.

Erweiterte Betriebssystemunterstützung: Verwalten Sie Ihre heterogene Serverumgebung mit einer integrierten Konsole. Neben der Möglichkeit, Windows 2000- und 2003-Server zu verwalten, bietet System Manager Unterstützung für mehrere unterschiedliche Linux- und Unix-Systeme:

- Red Hat Enterprise Linux v3 (ES) 32-Bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-Bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-Bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32-Bit - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32-Bit - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32-Bit - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2
- SUSE* Linux Server 9 ES 32-Bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Ansicht "Geplanter Task": Anzeigen aller geplanten oder abgeschlossenen Agentenbereitstellungs-, Erkennungs-, Software-Update- und benutzerdefinierte Skripte-Tasks

über eine zentrale Konsole. Sie können jeden Task neu planen, ändern oder als periodisch auszuführende Aktion konfigurieren.

Intel* AMT-Unterstützung: Unterstützung für Intel* Active Management Technology, Versionen 1 und 2. Mit Intel AMT können Sie vernetzte Geräte in jedem beliebigen Zustand aus der Ferne verwalten (unter Verwendung von Out-of-Band (OOB)-Kommunikation), selbst wenn das Betriebssystem des Geräts nicht reagiert oder ausgeschaltet ist. Zu den einzigen Voraussetzungen gehört, dass das Gerät mit einem Unternehmensnetzwerk verbunden ist und über Standby-Strom verfügt.

IPMI-Unterstützung: Das Produkt unterstützt Intelligent Platform Management Interface (IPMI)-kompatible Server (Versionen 1.5 oder 2.0), inklusive Out-of-Band Remote-Wiederherstellung nach einem Serverabsturz und das Anzeigen autonomer Verwaltungsdaten, selbst wenn Betriebssystem oder Prozessor nicht laufen.

Tool für die Skripterstellung: Sie können benutzerdefinierte Tasks auf Geräten ausführen, indem Sie Skripte für den lokalen Scheduler erstellen.

Leistungsüberwachung: Sie können die Echtzeitleistung Ihrer verwalteten Enterprise- oder Blade-Server mithilfe einer Vielzahl von Attributen überwachen. Sie können diese Attribute sogar nachverfolgen lassen und Verlaufsdaten zur Leistung durchsehen, die über einen Zeitraum von mehreren Tagen erfasst wurden. Sie können Geräte überwachen, auf denen der Überwachungsagent installiert ist, und Sie können Out-of-Band IPMI-aktivierte Server ohne Agent überwachen.

Unterstützung für Blade-Server: IBM-Blade-Gehäuse und Server-Blades werden unterstützt, einschließlich Erkennung, Gehäuseidentifizierung, Inventar, und Patch-Management. Zur Optimierung des Datenerfassungsvorgangs gibt Ihnen das Produkt die Möglichkeit, Blades nach Funktion, Gehäuse, Rack oder anderen Kriterien zu gruppieren.

Berichte: Sie können für jedes Gerät in der Datenbank Berichte ausführen, die Nutzungsstatistiken enthalten und über Ressourcenzuordnungen sowie zahlreiche andere Messungen informieren. Dieses Produkt beinhaltet mehrere vordefinierte Berichte. Diese Berichte werden im Handumdrehen erstellt, da sie direkt auf die Informationen in der Datenbank zugreifen und Daten als zwei- oder dreidimensionale Torten- und Balkengrafiken aufbereiten. Mithilfe benutzerdefinierter Abfragen können Sie zusätzliche Berichte erstellen.

Zustandsüberwachung/Alarme: Die Überwachung des Gesamtzustands eines Geräts ist einfach. Sie können Grenzwerte für Überwachungsdaten wie Festplattenspeicher- oder CPU-Nutzung definieren und festlegen, wie Sie bei einer Überschreitung eines Grenzwertes benachrichtigt werden möchten. Sie können sich über einen bedenklichen Serverzustand informieren und Gegenmaßnahmen einleiten, um das Problem zu lösen, bevor Benutzer mit dem Problem konfrontiert werden oder Ausfallzeiten in Kauf genommen werden müssen.

Software-Updates: Sie können Software-Updates für System Manager und für Intel* Hardware beziehen. Sie können die ausgewählten Updates mithilfe der Softwareverteilungsfunktionen manuell bereitstellen.

Rollenbasierte Administration: Fügen Sie Benutzer hinzu und konfigurieren Sie den Zugriff dieser Benutzer auf Tools und andere Geräte auf der Basis ihrer administrativen Rolle. In der rollenbasierten Administration weisen Sie Bereiche zu, um festzulegen, welche Geräte ein

Benutzer anzeigen und verwalten kann, und Sie erteilen Rechte, mit denen gesteuert wird, welche Tasks Benutzer ausführen können, beispielsweise Berichterstellung.

Inventar: Mithilfe des Inventarscanners liest das Produkt umfassende Informationen zur Hardware und Software in die Core-Datenbank. Sie können diese Daten dann anzeigen, drucken und exportieren.

Geräteerkennung: Stellen Sie sicher, dass Sie über den Inhalt Ihres Netzwerks jederzeit genau informiert sind. Die Geräteerkennung erfasst einfache Informationen zu allen Geräten in Ihrer Umgebung und sorgt damit für mehr Kontrolle und schnellere Bereitstellung von Agenten auf Zielgeräten.

Unterstützung für Active System Console: Unterstützung für die Active System Console, die einen schnellen Gesamteindruck vom Systemzustand bietet, wenn Sie den Active System Console-Agenten auf einem Gerät installieren. Sie erkennen auf einen Blick, ob die ausgewählten Hardwareelemente wie vorgesehen funktionieren und ob sich Probleme abzeichnen, denen Sie ggf. Aufmerksamkeit schenken müssen. Des Weiteren können Sie detaillierte Leistungsdaten des Systems und eine Aufstellung der Systemkomponenten anzeigen, einschließlich Hardware, Software, Protokolle und Informationen zu Intel* AMT und IPMI (sofern das Gerät eine dieser beiden Technologien unterstützt).

Executive Dashboard: Mehrere Tools (Informationsdiagramme, Schaubilder, Zeiger und Messinstrumente), mit denen sich der Zustand oder Status der Unternehmensumgebung überwachen lässt.

Hilfe: Dieses Produkt enthält ein Erste Schritte-Kapitel sowie kontextbezogene Hilfethemen.

Bedeutung wichtiger Produktbegriffe

- **Core Server:** Der Mittelpunkt einer Verwaltungsdomäne. Alle Schlüsseldateien und Dienste des Produkts befinden sich auf dem Core Server. Eine Verwaltungsdomäne besitzt nur einen Core Server. Ein Core Server kann ein neuer Server sein oder ein Server, der einem neuen Zweck zugeführt wird.
- **Konsole:** Die Browser-basierte Konsole ist die zentrale Benutzeroberfläche des Produkts.
- Core-Datenbank:Das Produkt erstellt eine MSDE-Datenbank auf dem Core Server, um Verwaltungsdaten zu speichern.
- **Verwaltete Geräte:** Geräte in Ihrem Netzwerk, auf denen Produktagenten installiert sind. Mit "Geräte" sind Desktops, Server, Laptops/mobile Computer, Blade-Gehäuse usw. gemeint. Ein Core Server kann mehrere Tausend Geräte verwalten.
- **Öffentlich:** Elemente (z. B. Gruppen, Verteilungspakete oder Tasks), die für alle Benutzer sichtbar sind. Wenn ein Benutzer ein öffentliches Element ändert, bleibt die Änderung öffentlich. Öffentliche Gruppen werden von Benutzern mit Administratorrechten erstellt.
- **Privat** oder **Benutzer:** Elemente, die vom gegenwärtig angemeldeten Benutzer erstellt werden. Sie sind für andere Benutzer nicht sichtbar. Private Elemente oder Benutzerelemente werden unter den Strukturen **Eigene Verteilungsmethoden, Eigene Pakete** und **Eigene Tasks** angezeigt. Benutzer mit Administratorrechten können private Gruppen und Benutzerpakete und -tasks anzeigen.

- **Global:** Ein für andere Benutzer sichtbares Element. Wenn ein Benutzer Eigentümer eines globalen Elements wird (indem er es modifiziert), verzweigt es in zwei Elemente: Das globale Element verbleibt am Speicherort, während ein Benutzerelement im Ordner "Benutzer" gespeichert wird. Die Benutzerinstanz des Elements ist für andere Benutzer nicht mehr sichtbar. Ein Benutzer kann jeden sichtbaren Task als global markieren und ihn auf diese Weise mit anderen Benutzern teilen. Sobald ein Benutzer die Option "Global" der Eigenschaften des Elements deaktiviert, ist der Task nur noch in der Gruppe "Benutzertasks" des Benutzers sichtbar.

Erste Schritte

Übersicht

Willkommen bei LANDesk® System Manager! Diese Standalone-Anwendung für die Geräteverwaltung unterstützt Sie gezielt und effizient bei der Verwaltung Ihrer Geräteumgebung und hilft Ihnen, Ihre wertvolle Zeit optimal zu nutzen. Diese Vorteile machen sich für Ihr Unternehmen in einer deutlicheren Reduzierung des Zeit- und Kostenaufwands bezahlt. Mit System Manager können Sie Geräte zentral verwalten und für die Durchführung von Aktionen wie Power Cycling, Anfälligkeitsanalysen oder das Konfigurieren von Alarmen zu Gruppen zusammenfassen. Darüber hinaus können Sie mit System Manager Probleme an entfernten Standorten lösen, Ihr Netzwerk schützen und die Geräte mithilfe aktueller Patches auf dem neuesten Stand halten.

Dieses Handbuch zielt darauf ab, Sie so schnell wie möglich mit System Manager vertraut zu machen, indem Sie Dienste konfigurieren, die Konsole ausführen, Geräte erkennen, Geräte in die Liste Eigene Geräte verschieben und verwaltete Geräte für auf ihnen auszuführende Aktionen konfigurieren.

System Manager ist eine Webanwendung, auf die Sie mit Ihrem Browser zugreifen und auf diese Weise Ihre Server von einer Remote-Arbeitsstation aus verwalten können. Sie verhält sich wie viele der Webanwendungen, mit denen Sie ggf. bereits vertraut sind, jedoch verfügt sie über mehrere erweiterte Windows-ähnliche Steuerelemente, die die Anwendung benutzerfreundlicher machen. Zeigen Sie beispielsweise mit dem Mauszeiger auf ein Steuerelement und doppelklicken Sie dann auf dieses Element oder klicken Sie mit der rechten Maustaste darauf (so wie in einer Windows-Anwendung). Beispiel: Sie können in der Liste Eigene Geräte auf einen

Gerätenamen doppelklicken, um auf die spezifischen Informationen zu diesem Gerät zuzugreifen, oder Sie können mit der rechten Maustaste klicken, um verfügbare Aktionen anzuzeigen.

In den folgenden Schritten wird beschrieben, wie Sie System Manager in Betrieb nehmen, Geräte in Ihrem Netzwerk erkennen lassen, die in die Liste Eigene Geräte zu verschiebenden Server auswählen, Agenten bereitstellen und die Geräte dann als Ziel für die Bearbeitung mit unterschiedlichen Tasks auswählen.

Ausführen des Installationsprogramms

Wählen Sie während der Installation auf der Autorun-Seite LANDesk® System Manager aus. Genaue Anweisungen finden Sie unter Stufe 2 des Installations- und Bereitstellungshandbuchs.

Sobald Sie System Manager installiert haben, steht der Verwendung des Produkts nichts mehr im Wege. In den nachstehenden Abschnitten machen wir Sie mit mehreren obligatorischen Schritten vertraut: Ausführen des Core-Aktivierungsprogramms, Konfigurieren von Diensten, Erkennen von Computern, Isolieren der aktiv zu verwaltenden Geräte durch Verschieben der Geräte in die Liste Eigene Geräte, Gruppieren von Geräten, Hinzufügen von Benutzern und Bereitstellen von Agenten. Sobald diese Aufgaben abgeschlossen sind, sind Sie bereit, die leistungsstarken und zuverlässigen Funktionen von System Manager kennenzulernen und zur Verwaltung Ihrer Geräte einzusetzen.

Aktivieren des Core Servers

Sie können das Produkt erst ausführen, nachdem Sie den Core Server aktiviert haben.

Verwenden Sie das Core Server-Aktivierungsprogramm für folgende Aufgaben:

- Erstmalige Aktivierung eines neuen System Manager Core Servers.
- Aktualisieren eines vorhandenen System Manager Core Servers oder Aktualisierung auf Management Suite oder System Manager

Jeder Core Server benötigt ein eindeutiges Autorisierungszertifikat.

Dieses Dienstprogramm wird beim ersten Neustart automatisch ausgeführt.

Verbinden Sie den Core Server mit dem Internet und führen Sie folgende Schritte aus:

1. Klicken Sie auf Start | Alle Programme | Core Server-Aktivierung.
2. Geben Sie den eindeutigen Benutzernamen und das Kennwort ein, das Ihnen beim Erwerb Ihrer Lizenzen zur Verfügung gestellt wurde.
3. Klicken Sie auf Aktivieren.

Der Core kommuniziert mit dem Software-Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte Proxy und geben die erforderlichen Proxy-Informationen ein. Wenn Ihr Core mit dem Internet verbunden ist, wird die Kommunikationsverbindung mit dem Lizenzserver automatisch, d.h. ohne Ihr Eingreifen, hergestellt. Wenn keine Verbindung mit dem Core besteht, klicken Sie beim Neustart auf Schließen und senden die Autorisierungsdatei an licensing@landesk.com.

Der Core Server hinterlegt in regelmäßigen Abständen Verifizierungsdaten zur Knotenzahl in der Datei "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Diese Datei wird in regelmäßigen Abständen an den LANDesk Software-Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den Software-Lizenzserver ungültig.

- Das Core Server-Aktivierungsprogramm startet keine DFÜ-Verbindung automatisch. Wenn Sie die DFÜ-Verbindung jedoch manuell starten und dann das Aktivierungsprogramm ausführen, kann das Programm die Daten zur Nutzung auch über eine DFÜ-Verbindung weiterleiten.
- Sie können den Core Server auch per E-Mail aktivieren. Senden Sie die Datei mit der Erweiterung .TXT, die Sie unter Programme\LANDesk\Authorization finden, an licensing@landesk.com. Der Kundensupport von LANDesk beantwortet die E-Mail mit einer Datei und mit Anweisungen zum Kopieren der Datei auf den Core Server. Dieser Vorgang bildet den Abschluss des Aktivierungsprozesses.

Hinzufügen von Benutzern

System Manager Benutzer sind Benutzer, die sich an der Konsole anmelden und bestimmte Aufgaben für bestimmte Geräte im Netzwerk ausführen können. Sie werden mithilfe der rollenbasierten Administrationsfunktion verwaltet. Mithilfe der rollenbasierten Administration können Sie Benutzern des Produkts, abhängig von ihren Rechten und ihrem Bereich, administrative Rollen zuweisen. Die Rechte legen fest, welche Produkt-Tools und -Funktionen der Benutzer sehen und verwenden kann. Der Bereich bestimmt, welche Geräte der Benutzer sehen und verwalten kann. Sie können eine Vielzahl von unterschiedlichen Benutzern erstellen und deren Rechte und Bereiche an Ihre Verwaltungsanforderungen anpassen. Sie können beispielsweise einen Benutzer erstellen, der die Help Desk-Aufgabe wahrnimmt, indem Sie diesem Benutzer die für diese Rolle erforderlichen Rechte erteilen. Zu diesem Thema finden Sie ausführliche Informationen im Kapitel "Rollenbasierte Administration" desSystem Manager Benutzerhandbuchs.

Beim Installieren des Produkts werden automatisch zwei Benutzerkonten erstellt (siehe unten). Sie können nach Bedarf weitere Benutzer manuell hinzufügen. Benutzer werden nicht in der Konsole erstellt. Sie werden stattdessen in der Gruppe "Benutzer" angezeigt (im linken Navigationsfenster auf Benutzer klicken), nachdem sie der LANDesk Management Suite-Gruppe in der Windows NT-Benutzerumgebung auf dem Core Server hinzugefügt wurden. Die Gruppe "Benutzer" zeigt alle Benutzer an, die gegenwärtig in der LANDesk Management Suite-Gruppe auf dem Core Server vorhanden sind.

Die Gruppe "Benutzer" umfasst zwei Standardbenutzer. Einer dieser beiden Benutzer ist der Standard-Administrator. Dies ist der Administrator, der während der Installation des Produkts am Server angemeldet war.

Der andere Benutzer ist der Standardvorlagenbenutzer.Dieser Benutzer verfügt über eine Vorlage mit Benutzereigenschaften (Rechte und Bereich), die zum Konfigurieren neuer Benutzer verwendet wird, wenn diese der Management Suite-Gruppe hinzugefügt werden. Wenn Sie also dieser Gruppe in der Windows NT-Umgebung einen Benutzer hinzufügen, erbt der Benutzer die Rechte und Bereiche, die aktuell in den Eigenschaften "Standardvorlagenbenutzer" definiert sind. Wenn Sie für den Standardvorlagenbenutzer alle Rechte und den "Standardbereich: Alle Rechner" ausgewählt haben, wird jeder neue Benutzer der LANDesk Management Suite-Gruppe

der Gruppe "Benutzer" hinzugefügt (mit Rechten für alle Produkttools und mit Zugriff auf alle Geräte).

Sie können die Eigenschaftseinstellungen für den "Standardvorlagenbenutzer" ändern, indem Sie ihn auswählen und auf Bearbeiten klicken. Wenn Sie z.B. eine große Anzahl von Benutzern gleichzeitig hinzufügen möchten, von denen jedoch nicht alle Zugriff auf alle Tools oder Geräte haben sollen, ändern Sie zuerst die Einstellungen für den "Standardvorlagenbenutzer" und fügen dann die Benutzer zur LANDesk Management Suite-Gruppe hinzu (siehe unten beschriebene Schritte). Der "Standardvorlagenbenutzer" kann nicht entfernt werden.

Wenn Sie einen Benutzer zur LANDesk Management Suite-Gruppe in Windows NT hinzufügen, wird der Benutzer automatisch in die Gruppe "Benutzer" im Fenster Benutzer eingelesen und übernimmt dieselben Rechte und denselben Bereich wie der aktuelle "Standardvorlagenbenutzer". Es werden der Name, der Bereich und die Rechte des Benutzers angezeigt. Zusätzlich werden neue (nach der eindeutigen Anmelde-ID des Benutzers) benannte Benutzeruntergruppen in den Gruppen "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripte" erstellt (beachten Sie, dass NUR ein Administrator Benutzergruppen anzeigen kann).

Umgekehrt wird ein Benutzer, den Sie aus der LANDesk Management Suite-Gruppe entfernen, nicht mehr in der Liste Benutzer angezeigt. Das Konto des Benutzers existiert weiterhin auf dem Core Server und kann jederzeit wieder der LANDesk Management Suite-Gruppe hinzugefügt werden. Außerdem bleiben die Benutzeruntergruppen unter "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripte" erhalten, sodass Sie den Benutzer, ohne dessen Daten zu verlieren, wiederherstellen und Daten in andere Benutzer kopieren können.

Aktualisieren Sie den Frame Benutzerin der System Manager-Konsole, indem Sie die F5-Taste drücken. Um zu erfahren, wie Sie der LANDesk Management Suite-Gruppe einen Benutzer oder eine Domänengruppe hinzufügen oder ein neues Benutzerkonto erstellen, lesen Sie die Ausführungen unter "Hinzufügen von Produktbenutzern" die Ausführungen unter "Rollenbasierte Administration" im System Manager *Benutzerhandbuch*.

So fügen Sie einen Benutzer oder eine Domänengruppe der LANDesk Management Suite-Gruppe hinzu

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Gruppen** des Servers.
2. Klicken Sie mit der rechten Maustaste auf die **LANDesk Management Suite-Gruppe** und klicken Sie dann auf **Zur Gruppe hinzufügen**.
3. Klicken Sie auf **Hinzufügen**, geben Sie dann mindestens einen Benutzer ein bzw. wählen Sie mindestens einen Benutzer aus der Liste aus.
4. Klicken Sie auf **Hinzufügen** und dann auf **OK**.

Hinweis: Sie können der LANDesk Management Suite-Gruppe auch einen Benutzer hinzufügen, indem Sie mit der rechten Maustaste auf das Benutzerkonto in der Liste **Benutzer** klicken und dann auf **Eigenschaften | Mitglied von** sowie anschließend auf **Hinzufügen** klicken, um die Gruppe auszuwählen und den Benutzer hinzuzufügen.

Wenn noch keine Benutzerkonten auf dem Server existieren, müssen Sie sie erst erstellen.

So erstellen Sie ein neues Benutzerkonto

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppe | Benutzer** des Servers.
2. Klicken Sie mit der rechten Maustaste auf **Benutzer** und klicken Sie dann auf **Neue Benutzer**.
3. Geben Sie im Dialogfeld **Neuer Benutzer** einen Namen und ein Kennwort ein.
4. Legen Sie die Kennworteinstellungen fest.
5. Klicken Sie auf **Erstellen**. Das Dialogfeld **Neuer Benutzer** bleibt geöffnet, sodass Sie zusätzliche Benutzer erstellen können.
6. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Fügen Sie den Benutzer zur LANDesk Management Suite-Gruppe hinzu, damit er in der Gruppe "Benutzer" in der Konsole angezeigt wird.

Konfigurieren von Diensten und Berechtigungsnachweisen

Bevor Sie Geräte in Ihrem Netzwerk verwalten können, müssen Sie System Manager die erforderlichen Anmeldeinformationen zur Verfügung stellen. Geben Sie mithilfe des Dienstprogramms "Dienste konfigurieren" auf dem Core (SVCCFG.EXE) die erforderlichen Betriebssystem-, Intel* AMT- und IPMI BMC-Anmeldeinformationen an. Sie können außerdem zusätzliche Einstellungen angeben, beispielsweise Inventarstandards, PXE-Warteschlangeneinstellungen und LANDesk-Datenbankeinstellungen.

Verwenden Sie "Dienste konfigurieren", um Folgendes zu konfigurieren:

- Datenbankname, Benutzername und Kennwort. (Während der Installation festgelegt.)
- Anmeldeinformationen für das Planen von Jobs für verwaltete Geräte. (Sie können mehr als einen Satz Administratorberechtigungsnachweise eingeben.)
- Anmeldeinformationen zum Konfigurieren von IPMI BMCs. (Sie können nur einen Satz BMC-Berechtigungsnachweise eingeben.)
- Anmeldeinformationen zum Konfigurieren Intel AMT-kompatibler Geräte. (Sie können nur einen Satz Intel AMT-Anmeldeinformationen eingeben.)
- Scanintervall der Serversoftware, Wartung, Tage, die Inventarscans gespeichert bleiben, und Länge des Anmeldeprotokolls.
- Handhabung doppelt vorhandener Gerätekennungen.
- Scheduler-Konfiguration, einschließlich des Intervalls zwischen geplanten Aufträgen und Abfrageevaluierungen
- Benutzerdefinierte Auftragskonfiguration, einschließlich Timeout für die Remote-Ausführung.

1. Klicken Sie auf dem Core Server auf Start | Alle Programme | LANDesk | LANDesk - Dienste konfigurieren.
2. Klicken Sie auf die Registerkarte Scheduler.
3. Klicken Sie auf Anmeldung ändern.
4. Geben Sie die Anmeldeinformationen ein, die der Dienst auf den verwalteten Geräten verwenden soll, für gewöhnlich ein Domänenadministratorkonto.
5. Klicken Sie auf Hinzufügen. Fügen Sie nach Bedarf weitere Anmeldeinformationen hinzu, wenn nicht auf allen verwalteten Geräten dieselben Administrator-Benutzernamenkonten aktiviert sind.

6. Klicken Sie auf Übernehmen.
7. Wenn es in Ihrer Umgebung IPMI-kompatible Server gibt, klicken Sie auf die Registerkarte BMC-Kennwort. Geben Sie ein Kennwort in das Textfeld Kennwort ein, geben Sie das Kennwort in das Textfeld Kennwort bestätigen erneut ein und klicken Sie dann auf OK. (Alle verwalteten IPMI-Server müssen denselben BMC-Benutzernamen und dasselbe BMC-Kennwort verwenden.)
8. Klicken Sie bei Intel AMT-aktivierten Geräten auf die Registerkarte Intel AMT-Konfiguration. Geben Sie den gegenwärtig konfigurierten Intel AMT-Benutzernamen in das Textfeld Benutzername und das aktuell konfigurierte Kennwort in das Textfeld Kennwort ein. Geben Sie das Kennwort erneut in der Textfeld Kennwort bestätigen ein und klicken Sie auf OK.
9. Definieren Sie nach Bedarf weitere Einstellungen, beispielsweise das Softwarescan-Intervall.
10. Klicken Sie auf OK, um die Änderungen zu speichern.

Klicken Sie auf **Hilfe** auf der jeweiligen Registerkarte "Dienste konfigurieren", um weitere Informationen zu erhalten.

Ausführen der Konsole

Mit dem umfassenden Tool-Angebot von System Manager können Sie die in Ihrem Netzwerk installierten Geräte anzeigen, konfigurieren, verwalten und schützen. Die Konsole ist der Zugriffspunkt für die Verwendung dieser Tools.

Im oberen Fensterausschnitt der Konsole sehen Sie den Server, bei dem Sie angemeldet sind, und den Benutzer, unter dem Sie sich angemeldet haben. Die Liste Eigene Geräte ist das Hauptfenster der Konsole und der Ausgangspunkt für die meisten Funktionen. Im linken Fensterausschnitt sind die verfügbaren Tools zu sehen. Im rechten Bereich der Konsole werden Dialogfelder und Bildschirme angezeigt, die zur Durchführung von Verwaltungsaufgaben dienen.

Der Vorteil der Konsole liegt darin, dass Sie ihre gesamten Funktionen aus der Ferne - beispielsweise von Ihrer Arbeitsstation aus - ausführen können; das heißt, Sie sparen sich zusätzliche Wege zum Serverraum oder müssen nicht mehr jedem einzelnen Gerät einen Besuch abstatten, um routinemäßige Wartungsaufgaben auszuführen oder Probleme zu beheben.

Es gibt drei Möglichkeiten, die Konsole zu starten:

- Klicken Sie auf dem Core Server auf Start | Alle Programme | LANDesk | System Manager.
- Geben Sie in einem Browser an einer Remote-Arbeitsstation die URL http://coreserver/LDSM ein.

Erkennen von Geräten

Verwenden Sie die Registerkarte **Erkennungskonfigurationen**, um neue Erkennungskonfigurationen zu erstellen, vorhandene Konfigurationen zu bearbeiten und zu löschen und eine Konfiguration für einen Erkennungsvorgang zu planen. Jede Erkennungskonfiguration besteht aus einem beschreibenden Namen, den zu scannenden IP-Bereichen und dem Erkennungstyp.

Nachdem Sie eine Konfiguration erstellt haben, können Sie mit dem Dialogfeld **Erkennung planen** festlegen, wann sie ausgeführt werden soll.

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Klicken Sie auf der Registerkarte **Erkennungskonfigurationen** auf die Schaltfläche **Neu**.
3. Füllen Sie die unten beschriebenen Felder aus. Klicken Sie, nachdem Sie alle Daten eingegeben haben, auf die Schaltfläche **Hinzufügen** und dann auf **OK**.

Im Folgenden werden die einzelnen Abschnitte des Dialogfelds **Erkennungskonfiguration** beschrieben.

- **Konfigurationsname:** Geben Sie einen Namen für die Konfiguration ein. Geben Sie der Konfiguration einen einprägsamen Namen, den Sie sich leicht merken können. Die Konfiguration kann bis zu 255 Zeichen umfassen; folgende Zeichen sind unzulässig: **"**, **+**, **#**, **&** oder **%**. Der Konfigurationsname wird nach Verwendung eines dieser Zeichen nicht mehr angezeigt.
- **Standard-Netzwerkscan:** Diese Option sucht nach Geräten, indem sie ICMP-Pakete an die IP-Adressen in dem von Ihnen angegebenen Bereich sendet. Diese Suche ist am gründlichsten, verursacht jedoch auch den größten Zeitaufwand. Diese Option verwendet standardmäßig NetBIOS, um Informationen zum Gerät zu sammeln.

  Die Scanoption des Netzwerks verfügt über einen **IP-Fingerabdruck**, mit dem die Geräteerkennung versucht, den Betriebssystemtyp über TCP-Paketantworten ausfindig zu machen. Der IP-Fingerabdruck verlangsamt die Erkennung geringfügig.

  Die Scanoption des Netzwerks verfügt darüber hinaus über die Option **SNMP verwenden** , mit der Sie den Scan für die Verwendung von SNMP konfigurieren können. Klicken Sie auf **Konfigurieren**, um Informationen zu Ihrer SNMP-Konfiguration einzugeben.
- **LANDesk CBA-Erkennung:** Sucht nach dem Standard Management Agent (der frühere Common Base Agent [CBA] in Management Suite) auf Geräten. Mit dem Standard Management Agent kann der Core Server nach Clients im Netzwerk suchen und mit ihnen kommunizieren. Diese Option erkennt Geräte, auf denen Produktagenten installiert sind. Router blockieren durch den Standard Management Agent und PDS2 bedingten Datenverkehr. Um eine Standard-CBA-Erkennung über mehrere Subnetze hinweg durchzuführen, muss der Router so konfiguriert sein, dass an mehrere Subnetze gerichtete Broadcasts unterstützt werden.

  Die CBA-Erkennungsoption verfügt zudem über eine **LANDesk PDS2-Erkennungsoption**, mit der die Geräteerkennung nach dem LANDesk Ping Discovery Service (PDS2) auf Geräten sucht. LANDesk Softwareprodukte wie LANDesk® System Manager, Server Manager und LANDesk Client Manager verwenden den PDS2-Agenten. Wählen Sie diese Option aus, wenn es in Ihrem Netzwerk Geräte gibt, auf denen diese Produkte installiert sind. CBA-Erkennung wird für Linux-Rechner nicht unterstützt. Wenn Sie jedoch PDS2 auswählen, können Linux-Rechner, auf denen ein Agent installiert ist, erkannt werden.

- **IPMI:** Sucht nach IPMI-fähigen Servern. IPMI ist eine von Intel, ***** H-P,* NEC,* und Dell* entwickelte Norm, die die Nachrichten- und Systemschnittstelle für verwaltbare Hardwarebestandteile definiert. IPMI bietet Überwachungs- und Wiederherstellungsfunktionen, mit denen Sie auf diese Funktionen zugreifen können, ganz gleich, ob das Gerät eingeschaltet ist oder nicht, und in welchem Zustand das Betriebssystem sich befindet. Denken Sie daran, dass das Gerät nicht auf ASF-Pings reagiert, wenn der Baseboard Management Controller nicht konfiguriert ist. Das Produkt verwendet ASF-Pings zum Erkennen von IPMI. Das heißt, dass Sie das Produkt als normalen Computer erkennen lassen müssen. Beim Push-Bereitstellen des Clients durchsucht ServerConfig das System, erkennt das Gerät als IPMI und konfiguriert den BMC.
- **Servergehäuse:** Sucht nach Blade-Server Chassis Management Modules (CMMs). Die Blades in den Servern werden als normale Server erkannt.
- **Intel* AMT:** Sucht nach Geräten mit Intel Active Management Technology-Unterstützung.
- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Letzte IP-Adresse:** Geben Sie die Abschluss-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Subnetzmaske:** Geben Sie die Subnetzmaske für den IP-Adressbereich ein, den Sie überprüfen möchten.
- **Hinzufügen:** Fügt den IP-Adressbereich in die Warteschlange im unteren Abschnitt des Dialogfelds ein.
- **Löschen:** Löscht den Inhalt der IP-Adressbereich-Felder.
- **Bearbeiten:** Wählen Sie einen IP-Adressbereich in der Arbeitswarteschlange aus und klicken Sie auf **Bearbeiten**. Der Bereich wird in den Textfelder oberhalb der Arbeitswarteschlange angezeigt. Sie können den Bereich dort bearbeiten und den neuen Bereich zur Arbeitswarteschlange hinzufügen.
- **Entfernen:** Entfernt den ausgewählten IP-Adressbereich aus der Arbeitswarteschlange.
- **Alle entfernen:** Entfernt alle IP-Adressbereiche aus der Warteschlange.

Nachdem Sie einen Erkennungstask konfiguriert haben, können Sie nun damit beginnen, die mit Ihrem Netzwerk verbundenen Geräte ausfindig zu machen, indem Sie festlegen, wann der Erkennungstask ausgeführt werden soll.

Planen und Ausführen des Erkennungstasks

Klicken Sie auf die Schaltfläche Zeitplan auf der Registerkarte Geräte erkennen, um das Dialogfeld Erkennung planen zu öffnen. Planen Sie mithilfe dieses Dialogfelds, wann eine Erkennung ausgeführt wird. Sie können festlegen, dass ein Erkennungstask sofort, zu einem späteren Zeitpunkt oder anhand eines Zeitplans (als regelmäßig wiederkehrender Vorgang) ausgeführt wird. Sie können die Option jedoch auch so konfigurieren, dass die Erkennung nur einmal ausgeführt wird, d.h., ohne eine etwaige Wiederholung zu einem späteren Zeitpunkt.

Nachdem Sie einen Erkennungstask geplant haben, können Sie sich auf der Registerkarte Erkennungstasks über den Status der Erkennung informieren. Die Planung eines wiederholt ausführenden Erkennungstasks ist hilfreich, da ein solcher Task Geräte, die im Netzwerk neu hinzukommen, automatisch erkennt.

Das Dialogfeld Erkennung planen beinhaltet folgende Optionen.

- Ungeplant lassen: Verknüpft den Task nicht mit einem Plan, belässt ihn jedoch in der Liste Erkennungsfunktionen, damit er nach Bedarf zu einem späteren Zeitpunkt zur Verfügung steht.
- Jetzt starten: Führt den Task so bald wie möglich aus. Es kann bis zu einer Minute dauern, bevor der Task gestartet wird.
- Zum geplanten Zeitpunkt starten: Startet den Task zu der von Ihnen angegebenen Uhrzeit. Wenn Sie auf diese Option klicken, müssen Sie Folgendes eingeben:
  - Uhrzeit: Die Uhrzeit für den Taskbeginn.
  - Datum: Das Datum für den Beginn des Tasks. Je nach lokalem Standard ist die Datumsreihenfolge entweder Tag-Monat-Jahr oder Monat-Tag-Jahr.
  - Wiederholen alle: Wenn der Task wiederholt werden soll, wählen Sie Täglich, Wöchentlich oder Monatlich aus. Wenn Sie "Monatlich" wählen und das Datum nicht in allen Monaten existiert (beispielsweise der 31.), wird der Task nur in den Monaten ausgeführt, in denen das Datum existiert.

So planen Sie einen Erkennungstask

1. Klicken Sie im linken Navigationsfenster auf Erkannte Geräte.
2. Wählen Sie auf der Registerkarte Erkennungskonfigurationen die gewünschte Konfiguration aus und klicken Sie auf Planen. Konfigurieren Sie den Erkennungsplan und klicken Sie auf Speichern.
3. Überwachen Sie den Fortschritt der Erkennung auf der Registerkarte Erkennungstasks. Klicken Sie auf Aktualisieren, um den Status zu aktualisieren.
4. Klicken Sie nach Abschluss des Erkennungsvorgangs auf Nicht verwaltet, um alle erkannten Geräte oben unter Erkannte Geräte einzublenden (der Fensterausschnitt aktualisiert sich nicht automatisch).

Anzeigen erkannter Geräte

Erkannte Geräte werden im Fensterausschnitt Erkannte Geräte nach Gerätetyp sortiert. Der Ordner Computer wird standardmäßig angezeigt. Klicken Sie auf die Ordner im linken Fensterausschnitt, um Geräte in unterschiedlichen Kategorien anzuzeigen. Klicken Sie auf Nicht verwaltet, um alle Geräte anzuzeigen, die von der Erkennung zurückgegeben werden.

- Blade-Server-Gehäuse werden im Ordner Gehäuse angezeigt.
- Standard-Enterprise-Geräte werden im Ordner Computer angezeigt.
- Router und andere Geräte werden im Ordner Infrastruktur angezeigt.
- Intel AMT-kompatible Geräte werden im Ordner Intel AMT angezeigt.
- IPMI-fähige Server werden im Ordner IPMI angezeigt.
- Geräte, die keiner Kategorie angehören, werden im Ordner Andere angezeigt.
- Drucker werden im Ordner Drucker angezeigt.

Hinweis: Für bestimmte Linux-Server wird ein allgemeines "Unix" als Betriebssystemname (oder manchmal sogar "Andere") angezeigt. Beim Bereitstellen des Standard Management Agent aktualisieren diese Server ihren Eintrag für den Betriebssystemnamen in der Liste **Eigene Geräte** und zeigen ein vollständiges Inventar an. So zeigen Sie erkannte Server an

1. Klicken Sie im linken Fensterausschnitt der Seite Geräteerkennung auf Computer oder einen anderen Gerätetyp, den Sie anzeigen möchten. Die Ergebnisse werden im rechten Fensterausschnitt angezeigt.

2. Klicken Sie zum Filtern der Ergebnisse auf das Filtersymbol  , geben Sie mindestens einen Suchteil ein und klicken Sie auf Suchen.

Zuweisen von Namen

Bei einer Netzwerkscan-Erkennung geben manche Server einen leeren Knotennamen (oder Host-Namen) zurück. Dies passiert am häufigsten bei Servern, die Linux ausführen. Sie müssen dem Gerät einen Namen zuweisen, damit Sie es mit Verwalten in die Liste Eigene Geräte verschieben können.

1. Klicken Sie auf der Seite Geräteerkennung auf das Gerät, dessen Name leer ist. (Sie müssen auf den leeren Bereich in der Spalte mit den Knotennamen klicken.)
2. Klicken Sie auf Name zuweisen in der Symbolleiste.
3. Geben Sie den Namen ein und klicken Sie auf OK.

Wenn Sie einen Produktagenten auf einem Gerät installieren, scannt er automatisch den Hostnamen und aktualisiert die Core-Datenbank mit den korrekten Informationen.

Verschieben von Geräten in die Liste "Eigene Geräte"

Nach dem Erkennen von Geräten müssen Sie manuell die Zielgeräte auswählen, die Sie verwalten möchten und sie in die Liste Eigene Geräte verschieben. Durch das Verschieben der Geräts wird keine Software auf dem Gerät installiert. Die Geräte werden lediglich zum Abfragen, Gruppieren und Sortieren in der Liste Eigene Geräte zur Verfügung gestellt. Sie wählen bestimmte Geräte als "Ziel" für eine bestimmte Aktion aus; dieses Modell lässt sich mit dem "Einkaufswagenmodell" zahlreicher Webanwendungen vergleichen.

1. Klicken Sie in der Ansicht Erkannte Geräte auf das Gerät, das Sie in die Liste Eigene Geräte verschieben möchten. Mit UMSCHALT+Mausklick oder STRG+Mausklicken können Sie mehrere Geräte auswählen.
2. Klicken Sie auf die Schaltfläche Ziel. Falls diese Schaltfläche nicht zu sehen ist, klicken Sie in der Symbolleiste auf <<. Die Schaltfläche befindet sich ganz rechts. Oder klicken Sie mit der rechten Maustaste auf die ausgewählten Server und klicken Sie dann auf Ziel.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte Verwalten.
4. Wählen Sie die Option zum Verschieben ausgewählter Geräte in die Verwaltungsdatenbank oder zum Verschieben von Zielgeräten.
5. Klicken Sie auf Verschieben.

Durch Klicken auf Verschieben werden die Geräte in die Liste Eigene Geräte verschoben und die Gerätedaten in die Datenbank geschrieben. Sobald sich die Informationen in der Datenbank befinden, können Sie gefilterte Abfragen und Berichte erstellen (nach Gerätename, IP-Adresse oder Betriebssystem).

Gruppieren von Geräten für Aktionen

Es ist sinnvoll, Geräte zu Gruppen zusammenzufassen, beispielsweise nach Standort oder Funktion, damit Sie auf diesen Geräten Aktionen schneller ausführen können. Beispiel: Sie möchten die Prozessorgeschwindigkeit von Geräten eines bestimmten Standorts anzeigen.

1. Klicken Sie in der Liste Eigene Geräteauf Private Gruppenoder Öffentliche Gruppen und klicken Sie dann auf Gruppe hinzufügen.
2. Geben Sie einen Namen für die Gruppe in das Feld Gruppenname ein.
3. Klicken Sie auf den Gruppentyp, den Sie erstellen möchten.
    - Statisch: Geräte, die der Gruppe hinzugefügt wurden. Sie bleiben in der Gruppe, bis sie entfernt oder nicht mehr von Ihnen verwaltet werden.
    - Dynamisch: Geräte, die ein oder mehrere Kriterien erfüllen, die von einer Abfrage definiert wurden. Beispiel: Eine Gruppe kann alle Server beinhalten, die sich gegenwärtig in einem Warnzustand befinden. Sie bleiben in der Gruppe, solange sie die für die Gruppe definierten Kriterien erfüllen. Geräte werden automatisch dynamischen Gruppen hinzugefügt, wenn sie die Abfragekriterien der Gruppe erfüllen.
4. Klicken Sie abschließend auf OK.
5. Um Geräte einer statischen Gruppe hinzuzufügen, klicken Sie auf die Geräte im rechten Fensterausschnitt der Liste Eigene Geräte, klicken Sie auf Verschieben/Kopieren, wählen Sie die Gruppe aus und klicken Sie auf OK.

Konfigurieren von Geräten zum Verwalten mithilfe der Konsole

Das Erkennen der Geräte allein bedeutet noch nicht, dass diese Geräte einem zentralen Verwaltungsauftrag zugeordnet sind. Damit Sie Geräte vollständig mit der Konsole verwalten und Alarmmeldungen zum Zustand empfangen können, müssen Sie auf den betreffenden Servern Verwaltungsagenten installieren. Sie können die Standard-Agentenkonfiguration installieren (installiert alle Verwaltungsagenten) oder Sie können Ihre eigenen Agentenkonfigurationen anpassen, um sie auf Ihren Geräten zu installieren. (Die Agentenkonfiguration muss den Überwachungsagenten einschließen, um Warnmeldungen empfangen zu können.)

Verwaltungsagenten können mit einem der folgenden Verfahren installiert werden:

- Wählen Sie in der Liste Eigene Geräte Zielgeräte aus und planen Sie dann einen Konfigurationstask für Agenten, um Agenten über eine Fernsteuerungsverbindung auf den Geräten zu installieren. (siehe Schritte weiter unten)
- Erstellen Sie eine Zuordnung zur LDlogon-Freigabe des Cores (//coreserver/ldlogon) und führen Sie SERVERCONFIG.EXE aus. (Eine Beschreibung der hierfür erforderlichen Schritte finden Sie unter "Abrufen der Agenten mit einer Pull-Prozedur" im Kapitel "Installation und Konfiguration von Geräteagenten" des System Manager Benutzerhandbuchs)
- Erstellen Sie ein selbstextrahierendes Paket für die Geräteinstallation. Führen Sie dieses Paket lokal auf dem Gerät aus, um die Agenten zu installieren. Während dieses Vorgangs müssen Sie mit Administratorrechten angemeldet sein. (Eine Beschreibung der hierfür erforderlichen Schritte finden Sie unter "Installieren von Agenten mit einem Installationspaket" im Kapitel "Installation und Konfiguration von Geräteagenten" des System Manager Benutzerhandbuchs)

So stellen Sie den Agenten mit einer Push-Prozedur bereit

1. Wählen Sie Zielgeräte in der Liste Eigene Liste aus (wie oben unter "Verschieben von Geräten in die Liste "Eigene Geräte"" beschrieben)

2. Klicken Sie im linken Navigationsfenster auf Agentenkonfiguration, klicken Sie mit der rechten Maustaste auf die Konfiguration, die Sie mit einer Push-Prozedur bereitstellen möchten, und klicken Sie auf Task planen.
3. Klicken Sie im linken Fensterausschnitt auf Zielgeräte und klicken Sie dann auf die Schaltfläche Zielliste hinzufügen.
4. Klicken Sie auf Task planen, klicken Sie auf Jetzt starten, um den Task sofort zu starten, oder klicken Sie auf Später starten (und legen Sie Datum und Uhrzeit für den Start der Taskausführung fest) und klicken Sie auf Speichern.

Sie können den Taskstatus auf der Registerkarte Konfigurationstasks überprüfen.

Installieren von Linux-Serveragenten

Sie können Linux-Agenten und RPMs von einem Remote-Standort aus auf Linux-Servern bereitstellen und installieren. Ihr Linux-Server muss für diese Aufgabe richtig konfiguriert sein, da sie sich andernfalls nicht ausführen lässt. Hinweise zum ordnungsgemäßen Konfigurieren eines Linux-Servers finden Sie unter "Installieren von Serveragenten" im Kapitel "Installation und Konfiguration von Geräteagenten" des *System Manager Benutzerhandbuchs.*

Einrichten von Alarmen

Wenn Probleme oder andere Ereignisse auf einem Gerät auftreten (z. B. eine Verknappung der Speicherressourcen des Geräts) kann System Manager einen Alarm senden. Sie können diese Alarme an Ihre Anforderungen anpassen, indem Sie den Schweregrad oder Grenzwert, der den Alarm auslösen wird, auswählen. Alarmmeldungen werden an die Konsole gesendet und lassen sich für die Ausführung spezifischer Aktionen konfigurieren. Sie können Alarme für zahlreiche unterschiedliche Ereignisse oder potenzielle Probleme definieren. Das Produkt umfasst einen Standard-Alarmregelsatz, der beim Installieren der Überwachungskomponenten auf dem verwalteten Gerät installiert wird. Dieser Alarm-Regelsatz leitet Feedback zum Systemzustand an das Konsole weiter. Dieser Standardregelsatz schließt u.a. folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Leistungsüberwachung
- IPMI-Ereignisse (auf relevanter Hardware)

Weitere Informationen zur Alarmierung finden Sie im Kapitel "Alarmkonfiguration" des System Manager Benutzerhandbuchs.

Einrichten von Alarmen

Wenn Probleme oder andere Ereignisse auf einem Gerät auftreten (z.B. eine Verknappung der Speicherressourcen des Geräts) kann System Manager einen Alarm senden. Sie können diese Alarme an Ihre Anforderungen anpassen, indem Sie den Schweregrad oder Grenzwert, der den Alarm auslösen wird, auswählen. Alarmmeldungen werden an die Konsole gesendet und lassen sich für die Ausführung spezifischer Aktionen konfigurieren. Sie können Alarme für zahlreiche unterschiedliche Ereignisse oder potenzielle Probleme definieren. Das Produkt umfasst einen Standard-Alarmregelsatz, der beim Installieren der Überwachungskomponenten auf dem

verwalteten Gerät installiert wird. Dieser Alarm-Regelsatz leitet Feedback zum Systemzustand an das Konsole weiter. Dieser Satz Standardregeln schließt u.a. folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Leistungsüberwachung

Weitere Informationen zur Alarmierung finden Sie im Kapitel "Alarmkonfiguration" des System Manager *Benutzerhandbuchs*.

Wie geht´s weiter?

Sie haben Server Manager für den reibungslosen Betrieb konfiguriert. Dabei haben Sie nur einen Bruchteil der Funktionen kennengelernt, die in Server Manager zur Verfügung stehen (z. B. die Geräteerkennung und Agentenkonfiguration). In den Begleithandbüchern (*Installations- und Bereitstellungshandbuch* und *Benutzerhandbuch*) können Sie sich ausführlich über alle Funktionen des Produkts informieren. Zu diesen Funktionen gehören:

Software-Updates: Sorgen Sie für fortlaufende Patchsicherheit auf allen verwalteten Geräten in Ihrem Netzwerk. Sie können mit diesem Tool die folgenden sich wiederholenden Prozesse automatisieren: Verwaltung aktueller Anfälligkeitsinformationen, Analyse der Anfälligkeit der verschiedenen Betriebssysteme, die auf den verwalteten Geräten ausgeführt werden, Herunterladen der relevanten ausführbaren Patchdateien, Reparieren von Anfälligkeiten durch die Verteilung und Installation notwendiger Patches auf Geräten und die Überprüfung des Patch-Installationserfolges.

Alarmierung: Stellen Sie sicher, dass Sie benachrichtigt werden, wenn ein Gerät einen bestimmten Grenzwert erreicht. In Zusammenarbeit mit dem Überwachungsfunktion kann die Alarmierung mit unterschiedlichen Verfahren benachrichtigen. Wenn Sie beispielsweise informiert werden möchten, wenn der Speicher auf Ihren Geräten eine Kapazitätsauslastung von 95% erreicht hat, können Sie auswählen, wie Sie über das Eintreten dieses Zustands informiert werden (der Agent kann eine E-Mail- oder Pager-Nachricht senden, ein Gerät neu starten oder herunterfahren oder Informationen in das Alarmprotokoll schreiben).

Abfragen: Verwalten Sie Ihr Netzwerk, indem Sie anhand bestimmter System- oder Benutzerkriterien nach Geräten in der Core-Datenbank suchen und sie entsprechend organisieren. Sie können eine Abfrage an die Liste der verwalteten Geräte richten, um die Geräte zu extrahieren zu machen, die den von Ihnen angegebenen Kriterien entsprechen (beispielsweise alle Geräte der Hauptniederlassung oder alle mit einer Arbeitsspeicherkapazität von 256 KB RAMI); anschließend können Sie diese Geräte zu Gruppen zusammenfassen und Aktionen ausführen. Diese Gruppen können statisch (die Mitglieder der Gruppe können nur manuell verwaltet werden) oder dynamisch sein (die Mitgliederzusammensetzung ändert sich, wenn Geräte bestimmte Kriterien erfüllen oder nicht erfüllen).

Überwachung: Überwachen Sie den Systemzustand eines Geräts mithilfe der unterstützten Überwachungsverfahren (direkte ASIC-Überwachung, In-Band IPMI, Out-of-Band IPMI, CIM usw.). Mithilfe der Überwachungsfunktion können Sie zahlreiche unterschiedliche Datenkategorien überwachen, beispielsweise die Anwendungsnutzung, Betriebssystemereignisse, Prozesse und Dienste, Vergangenheitsdaten und Hardwaresensoren

(Lüfter, Spannung, Temperatur etc.). Die Alarmierung ist eine verwandte Funktion, die den Überwachungsagenten zur Initiierung von Alarmaktionen verwendet.

Berichte: Generieren Sie ein breites Spektrum an Spezialberichten, in denen kritische Informationen zu den verwalteten Geräten in Ihrem Netzwerk aufgezeichnet werden. Server Manager fügt mithilfe eines Inventarscanners Geräte (sowie erfasste Hardware- und Softwaredaten zu diesen Geräten) zur Core-Datenbank hinzu. Sie können diese Inventardaten von der Inventaransicht eines Geräts aus einsehen und drucken. Außerdem können Sie die Daten verwenden, um Abfragen zu definieren und Geräte zu Gruppen zusammenzufassen. Das Bericht-Tool nutzt diese gescannten Inventardaten zusätzlich, indem es die erfassten Daten in nützlichen Berichtformaten zusammenträgt und ordnet. Das kann sich beim Erfassen und Formatieren von Berichten zur vorschriftsmäßigen Nutzung als hilfreich erweisen.

Erkennung nicht verwalteter Geräte: Hiermit können Sie nach Geräten suchen, die nicht von der Konsole verwaltet werden. Das Identifizieren nicht verwalteter Geräte ist der erste Schritt für die Eingliederung neuer Geräte in ein verwaltetes System. Sie können einen Erkennungstask konfigurieren, der jeden Monat automatisch einen Scan zur Erkennung neuer Geräte ausführt.

Lizenzierung

Die Lizenzprozedur sorgt mithilfe eines fortlaufenden Autorisierungsprozesses dafür, dass Ihr Unternehmen die vertraglich vereinbarte Lizenzknotenzahl nicht überschreitet. Mit diesem Ansatz können Sie zudem mehrere Core Server unter einem definierten Benutzerkonto verwenden. Der Lizenzprozess setzt eine Backend-Datenbank ein, um Benutzerkonten zu erstellen und zu verwalten. Der Lizenzprozess ist eine einfache Anforderungs- und Antwortprozedur zwischen Core Server und Backend, die es dem Core ermöglicht, seine Aktivität für eine weitere Periode zu erneuern.

Wenn Sie das Produkt (oder ein Add-On-Produkt) nach einer Installation ausführen, können Sie eine Evaluierungslizenz für einen Testzeitraum auswählen oder einen Benutzernamen und ein Kennwort eingeben, um eine bei LANDesk Sales käuflich erworbene Lizenz zu aktivieren. Alle Core Server werden mit demselben Benutzernamen und Kennwort für das vorhandene Konto aktiviert.

Der Aktivierungsprozess ist im Wesentlichen für Evaluierungslizenzen und den Produkterwerb derselbe. Wenn das Gerät mit dem Internet verbunden ist, ist der Prozess ein einfacher Informationsaustausch. Wenn das Gerät nicht mit dem Internet verbunden ist, müssen Sie manuell eine Datei per E-Mail an LANDesk senden und die dann an Sie zurückgesandte Antwortdatei auf dem Core Server speichern. Der Aktivierungsprozess funktioniert wie folgt:

1. Der Benutzer startet das Core-Aktivierungsprogramm
2. Es wird eine Datei erstellt, die sowohl Server- als auch Verwendungsdaten enthält. Sie wird vom privaten Schlüssel des Cores signiert und mit dem öffentlichen Schlüssel von LANDesk verschlüsselt.
3. Wenn eine Internet-Verbindung vorhanden ist, kommuniziert der Core mit den LANDesk-Servern und lädt die Aktivierungsdatei herauf. Die Backend-Datenbank verarbeitet die Informationen und sendet die Aktivierungsdaten zurück, die daraufhin direkt in die Datenbank geschrieben werden.
4. Wenn keine Internet-Verbindung vorhanden ist, können Sie die Datei aus dem \Program Files\LANDesk\Authorization Files-Ordner per E-Mail an licensing@landesk.com senden.

Hinzufügen von Lizenzen

Die über die Konsole zur Verfügung gestellte Funktionalität ist an den Erwerb eines Lizenzschlüssels gebunden. Sie können einen neuen Lizenzschlüssel hinzufügen, um auf zusätzliche Funktionen zuzugreifen oder die Anzahl der Benutzer zu ändern. Während der Installation wird eine 45 Tage gültige Probelizenz generiert. Sobald Sie eine gültige Lizenz zur Konsole hinzufügen, wird die temporäre Lizenz gelöscht.

So fügen Sie einen Lizenzschlüssel hinzu

1. Klicken Sie im linken Navigationsfenster auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Lizenz**.
3. Klicken Sie unten im Bildschirm auf die Verknüpfung http:/www.landesk.com/contactus/.

Wenn die oben angegebene Verknüpfung nicht funktionsfähig ist, wurde das Sicherheitsniveau des Browsers möglicherweise nicht auf "Mittel" eingestellt. Sie sollten die Standardstufe für die

Internetsicherheit in Internet Explorer von "Hoch" in "Mittel" ändern (**Tools > Internetoptionen > Sicherheit > Internet > Standardstufe**).

Die Konsole

Starten der Konsole

So starten Sie die Konsole

1. Klicken Sie auf dem Core Server auf **Start | Alle Programme | LANDesk | LANDesk System Manager**.

   oder

   Öffnen Sie auf einer Remote-Arbeitsstation einen Browser und geben Sie die Adresse der Konsole ein. Verwenden Sie das Format http://*corename*/ldsm.

2. Geben Sie einen gültigen Benutzernamen und ein Kennwort ein.

   Halten Sie beim Herstellen einer Verbindung zu einem Remote-Core Server die üblichen Windows-Richtlinien für die Remote-Anmeldung ein (d. h., wenn der Benutzer ein lokaler Benutzer dieses Core Servers ist, geben Sie lediglich den Benutzernamen ein; wenn es sich hingegen um einen Domänenbenutzer handelt, geben Sie den Domänennamen\Benutzernamen ein).
3. Klicken Sie auf **OK**.

Wenn die Geräteliste und Schaltflächen beim Starten der Konsole nicht angezeigt werden, müssen Sie den Core Server aktivieren.

Informationen zum Dialogfeld für die Anmeldung in System Manager

Verwenden Sie dieses Dialogfeld, um die Konsole zu starten und eine Verbindung mit einem Core Server herzustellen.

- **Benutzername:** Identifiziert einen Benutzer. Es kann sich dabei um einen Administrator-Benutzer oder um einen beliebigen Produktbenutzertyp mit eingeschränktem Zugriff handeln (weitere Informationen finden Sie unter Rollenbasierte Administration). Dieser Benutzer muss ein Mitglied der LANDesk Management Suite-Gruppe auf dem Core Server sein. Wenn Sie eine Verbindung mit einem Remote-Core Server herstellen, geben Sie den Domänennamen und Benutzernamen ein.
- **Kennwort:** Das Kennwort des Benutzers.

Verwenden der Konsole

Mithilfe von Tools können Sie die vernetzten Geräte Ihres Unternehmens anzeigen, konfigurieren, verwalten und schützen — und das von einer einzigen zentralen Konsole aus. Sie können Software- oder Konfigurationseinstellungen aktualisieren, Hard- und Softwareprobleme diagnostizieren, und mithilfe der rollenbasierten Administration den Benutzerzugriff auf

Funktionen und Geräte steuern. Wenn Sie zudem auch andere LANDesk-Produkte verwenden, können Sie außerdem direkt von der Konsole aus eine Verbindung mit diesen Produkten herstellen.

Im oberen Fensterausschnitt der Konsole sehen Sie den Server, bei dem Sie angemeldet sind, und den Benutzer, unter dem Sie sich angemeldet haben. Die Liste **Eigene Geräte** ist das Hauptfenster der Konsole und der Ausgangspunkt für die meisten Funktionen. Im linken Fensterausschnitt sind die verfügbaren Tools zu sehen. Im rechten Fensterausschnitt der Konsole werden die Dialogfelder und Bildschirme angezeigt, mit denen Sie Geräte und Benutzer verwalten, Berichte anzeigen, Erkennungen ausführen und Abfragen erstellen und bearbeiten usw. Sie können die Größe der Fensterausschnitte und Spalten der Liste **Eigene Geräte** ändern. Wenn auf einem Gerät keine Agenten installiert sind, enthalten nur die Spalten "Name" und "IP-Adresse" Informationen. In einigen Fällen wird auch das Betriebssystem angezeigt.

System Manager stellt Windows-ähnliche Funktionalität in der benutzerfreundlichen und direkt zugänglichen Umgebung Ihres Webbrowsers zur Verfügung.

- Klicken Sie mit der rechten Maustaste auf ein Gerät in der Liste **Eigene Geräte**, um verfügbare Optionen für das Gerät anzuzeigen, beispielsweise "Ping" und "Ziel".
- Um mehrere aufeinander folgende Einträge in einer Liste auszuwählen, klicken Sie auf den ersten Eintrag, drücken und halten die **Umschalttaste** gedrückt und klicken dann auf den letzten Eintrag.
- Um mehrere nicht aufeinander folgende Einträge in einer Liste auszuwählen, drücken und halten Sie die **Strg**-Taste gedrückt und klicken dann auf jeden einzelnen auszuwählenden Eintrag.

Damit Dialogfelder und Fenster ordnungsgemäß angezeigt werden, muss die Website von System Manager der Liste mit den zulässigen Websites im Popup-Blocker des Browsers hinzugefügt werden.

Rollenbasierte Administration
Welche Geräte Sie in der Liste **Eigene Geräte** anzeigen und verwalten und welche Verwaltungstools Sie verwenden können, hängt von den Zugriffsrechten und dem Gerätebereich ab, die/der Ihnen vom Administrator zugewiesen wurde(n). Weitere Informationen finden Sie unter Rollenbasierte Administration.

In diesem Abschnitt erfahren Sie mehr über:

- Die Liste "Eigene Geräte"
- Gerätesymbole
- Kontextmenüs
- Verwenden von Tools
- Anzeigen von Geräteeigenschaften

Die Liste "Eigene Geräte"

Die Liste **Eigene Geräte** enthält die weiter unten beschriebenen Gruppen und Untergruppen. Zusätzlich zu diesen Gruppen können Sie, abhängig von Ihren Zugriffsrechten und Gerätebereichen, eigene Gruppen erstellen, die die Geräteverwaltung zusätzlich vereinfachen.

Alle Geräte

Die Liste **Alle Geräte** führt - basierend auf dem Bereich des Benutzers - in einer einfachen Aufstellung (keine Untergruppen) die Geräte des zurzeit angemeldeten Benutzers auf. Wenn eine Verbindung zu einem bestimmten Core Server besteht, kann der Administrator jedes Gerät sehen, das von diesem Core Server verwaltet wird. Produktbenutzer sind hingegen eingeschränkt und sehen nur die Geräte, die zu dem ihnen zugewiesenen Bereich gehören (ein Bereich basiert auf einer Datenbankabfrage oder einem Verzeichnisstandort).

Geräte, die Produktagenten ausführen (Standard Management Agent und Inventaragent), werden automatisch in der Liste **Alle Geräte** angezeigt, wenn diese vom Inventarscanner in die Core-Datenbank eingelesen werden. In der Regel wird dieser Scan zum ersten Mal während der ersten Gerätekonfiguration durchgeführt. Sobald ein Gerät in die Core-Datenbank gescannt wurde, gilt es als verwaltetes Gerät — d.h., es kann jetzt von diesem Core Server verwaltet werden. Weitere Informationen zum Einrichten von Geräten finden Sie unter Konfigurieren von Clientagenten.

Da die Gruppe **Alle Geräte** automatisch mithilfe eines Inventarscans gefüllt wird, müssen Sie möglicherweise nie manuell nach Geräten suchen. Um jedoch Geräte zu finden, die nicht bereits in der Core-Datenbank enthalten sind (oder um nicht verwaltete Geräte in die Servergruppe zu verschieben), können Sie mit dem Geräteerkennungstool das Netzwerk nach Geräten durchsuchen. Weitere Informationen hierzu finden Sie unter Verwenden der Erkennung.

Die Gruppe **Alle Geräte** stellt für jedes Gerät die nachstehend beschriebenen Informationen zur Verfügung. Doppelklicken Sie auf **Alle Geräte**, um die Liste zu öffnen.

- **Name:** Der Hostname des Geräts, z.B. der Windows*-Computername.
- **IP-Adresse:** Die IP-Adresse des Geräts.
- **Zustand:** Der System- und Verfügbarkeitsstatus des Geräts. Unterstützte Zustände sind u.a. "Normal", "Warnung" oder "Kritisch".
- **Agent:** Der aktuell auf dem Gerät ausgeführte Agent.
- **Gerätetyp:** Zeigt die auf dem Computer installierte Hardware an (Intel AMT, IPMI, ASIC oder IPMI Advanced).
- **Betriebssystem:** Das vom Gerät ausgeführte Betriebssystem.
- **Aktiv seit:** Gibt an, seit welchem Datum und welcher Uhrzeit der Computer unterbrechungsfrei gearbeitet hat (in der Zeitzone der Datenbank).

Wenn Sie ein Gerät auswählen, werden die Eigenschaften des Geräts im Fensterausschnitt **Eigenschaften** unterhalb der Geräteliste angezeigt. Im Fensterausschnitt **Eigenschaften** werden zahlreiche wichtige Geräteattribute aufgelistet:

- **Kennung:** Die Kennnummer des Geräts. Diese Nummer wird von der Reihenfolge bestimmt, in der das Gerät der Liste **Alle Geräte** hinzugefügt wurde.
- **IP-Adresse:** Die IP-Adresse des Geräts.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Das Gerätemodell.
- **Prozessorgeschwindigkeit:** Die Geschwindigkeit der Geräte-CPU.
- **Prozessortyp:** Der CPU-Typ des Geräts.

Von der Konsole aus können Sie das Gerät , ein ausführliches Inventar anzeigen, und das Gerät als Ziel für eine Aktion auswählen, beispielsweise eine Berichterstellung.

Durch Doppelklicken auf ein Gerät in der Liste **Alle Geräte** gelangen Sie zur Serverinformationskonsole. Diese Konsole enthält eine Geräteübersicht, Konfigurationsinformationen, Fernsteuerungsoptionen und Informationen zur Alarmkonfiguration.

Öffentliche Gruppen

In der Liste **Öffentliche Gruppen** werden Gerätegruppen angezeigt, die von einem Benutzer, der über Administratorrechte verfügt, erstellt wurden. Diese Gruppen sind für andere Benutzer sichtbar.

In dieser Liste werden auch Blade-Gehäuse-Gruppen aufgeführt, die automatisch erstellt werden, wenn ein Chassis Management Module (CMM) zur Liste der verwalteten Geräte hinzugefügt wird. Die Gruppe listet den CMM und jeden verknüpften Blade-Server auf, den Sie verwalten. Eine Gehäusegruppe lässt sich nicht auf die gleiche Weise bearbeiten wie eine Gruppe, die Sie selbst erstellt haben.

Gruppen können statisch oder dynamisch sein. Dynamische Gruppen enthalten Geräte, die definierte Filterkriterien erfüllen, beispielsweise Prozessorgeschwindigkeit, Betriebssystem des Geräts oder ein benutzerdefiniertes Attribut wie "Gerätetyp". Statische Gruppen enthalten eine festgelegte Liste mit Geräten, andere statische Gruppen oder dynamische Gruppen.

Private Gruppen

In der Liste **Private Gruppen** werden die Gerätegruppen angezeigt, die vom gegenwärtig angemeldeten Benutzer erstellt wurden. Private Gruppen sind für andere Benutzer nicht sichtbar und können somit von anderen Benutzern nicht verwendet werden.

Gerätesymbole

Gerätesymbole werden in der Liste **Alle Geräte** angezeigt und geben über den aktuellen Zustand eines jeden Geräts Auskunft. Sie können die Zustandsinformationen für jedes Gerät einzeln aktualisieren, indem Sie auf das betreffende Gerät in der Liste **Eigene Geräte** und dann auf die Schaltfläche **Aktualisieren** klicken.

In der folgenden Tabelle sind die möglichen Geräte- und Statussymbole sowie deren Bedeutung aufgeführt:

Symbol	Beschreibung
	Gerät mit Normalstatus
	Gerät mit Alarmstatus

Symbol	Beschreibung
	Gerät mit kritischem Status
	Gerät mit unbekanntem Status

Kontextmenüs

Für alle Elemente in der Konsole, einschließlich Gruppen, Geräte, Abfragen, geplante Tasks, Skripte usw., stehen Kontextmenüs (Kurzbefehlmenüs) zur Verfügung. Kontextmenüs ermöglichen den schnellen Zugriff auf die allgemeinen Tasks und wichtigen Informationen eines Elements.

Sie können das Kontextmenü eines Elements anzeigen, indem Sie mit der rechten Maustaste auf das Element klicken. Wenn Sie beispielsweise in der Liste **Eigene Geräte** mit der rechten Maustaste auf ein verwaltetes Gerät klicken, werden im Kontextmenü in der Regel folgende Optionen eingeblendet:

- **Aus Gruppe entfernen:** Entfernt das Element aus einer benutzerdefinierten Gruppe.
- **Ziel:**Verschiebt das ausgewählte Gerät in die Liste Zielgeräte. **Hinweis:** Wenn keine Zielgeräte in der **Zielliste** angezeigt werden, klicken Sie auf der Registerkarte **Zielgeräte** auf **Aktualisieren**.
- **Einen Ping-Test mit dem Gerät durchführen:** Stellt sicher, dass das Gerät eingeschaltet ist.
- **Tracert-Gerät:** Sendet einen Trace-Route-Befehl, um ein gesendetes und empfangenes Netzwerkpaket sowie die Anzahl von Hops anzuzeigen, die das Paket benötigt, um an sein Ziel zu gelangen.

Eine komplette Aufstellung der Kontextmenüs von allen Elementen der Konsole würde den Rahmen dieser Hilfe sprengen. Sie können sich jedoch über jedes einzelne Element informieren, indem Sie mit der rechten Maustaste auf das betreffende Element klicken und die verfügbaren Optionen anzeigen.

Verwenden von Tools

Tools werden im linken Fensterausschnitt zur Verfügung gestellt. Verwenden Sie die Pfeiltasten am oberen Rand des Fensterausschnitts, um alle Tools anzuzeigen.

Der Administrator sieht alle Tools im linken Navigationsfenster. Andere Benutzer sehen nur die Tools (Funktionen), auf die sie aufgrund der ihnen zugewiesenen Rechte Zugriff haben. Wenn ein Benutzer z. B. nicht über das Berichtsrecht verfügt, wird das Tool "Berichte" nicht im linken Navigationsfenster angezeigt.

Vollständige Liste der Tools:

- **Software-Updates:** Laden Sie relevante Update-Pakete herunter.

- **Skripte:** Erstellen und verwalten Sie Skripte.
- **Geplante Tasks:** Zeigen Sie alle Tasks (mit Ursprung "Agentenkonfiguration", "Anfälligkeiten", "Geräteerkennung", oder "Skripte") im Scheduler an.
- **Überwachung:** Überwachen Sie die Echtzeitleistung Ihrer verwalteten Geräte mit einem breiten Spektrum von Attributen.
- **Alarmierung:** Konfigurieren Sie Alarme, setzen Sie Grenzwerte und konfigurieren Sie die Maßnahmen, die das Produkt bei Überschreitung eines Grenzwertes ergreift.
- **Agentenkonfiguration:** Definieren Sie eine IPMI (Baseboard Management Controller)-, Linux- oder Windows-Agentenkonfiguration.
- **Geräteerkennung:** Suchen Sie im Netzwerk nach Geräten, die nicht in die Core-Datenbank gescannt wurden.
- **Protokolle:** Zeigt das Alarmprotokoll an. Dieses Protokoll zeigt die Alarme an, die Sie als diejenigen markiert haben, die auf Ihren verwalteten Geräten angezeigt werden sollen.
- **Berichte:** Verwalten Sie vordefinierte Berichte.
- **Abfragen:** Erstellen und ändern Sie an die Datenbank gerichtete Abfragen, um Geräte zu isolieren, die Ihre Kriterien erfüllen.
- **Benutzer:** Steuern Sie den Benutzerzugriff auf Geräte und Tools basierend auf den Rechten der Benutzer und der ihnen zugewiesenen Bereiche.
- **Voreinstellungen:** Erstellen Sie benutzerdefinierte Inventarattribute und zeigen Sie Lizenzinformationen an.
- **Hardwarekonfiguration:** Öffnen Sie ein separates Fenster, in dem Konfigurationsoptionen für Intel* AMT-Geräte angezeigt werden.

Wenn Sie auf den Namen eines Tools klicken, wird dessen Anzeige im rechten Fensterausschnitt geöffnet.

Anzeigen von Geräteeigenschaften

In der Ansicht **Eigene Geräte** können Sie im Handumdrehen Informationen zu einem Gerät anzeigen, indem Sie auf das Gerät in der Liste klicken und im unteren Fensterausschnitt **Eigenschaften** auswählen.

Genauere Informationen über das Gerät finden Sie in den Inventardaten des Geräts. Sie können Inventardaten in der Ansicht **Alle Geräte** anzeigen, indem Sie auf das Gerät klicken und die Registerkarte **Inventar anzeigen** im unteren Fensterausschnitt auswählen, um das Fenster **Inventar** vollständig zu öffnen.

Auswählen von Zielgeräten

Mithilfe der Liste **Zielgeräte** können Sie Tasks auf ausgewählten Geräten ausführen, beispielsweise Agenten auf einer ausgewählten Gruppe von Geräten bereitstellen oder einen Scan auf Software-Updates durchführen.

Es wird empfohlen, maximal 250 Geräte in die Liste aufzunehmen. Die Geräte bleiben in der Liste, bis Ihre Konsolensitzung abläuft (nach 20 Minuten Inaktivität).

Fügen Sie Geräte zur Liste **Zielgeräte** hinzu, indem Sie sie aus einer Geräteliste auswählen. Wenn die gewünschten Geräte nicht angezeigt werden, können Sie mit der Schaltfläche **Suchen** auf der Symbolleiste nach den Geräten suchen. Suchen Sie entweder nach einem bestimmten

Gerät oder nach mehreren Geräten gleichzeitig (mithilfe des Platzhalterzeichens % oder *). Klicken Sie auf die Symbolleistenschaltfläche **Ziel**, um das Gerät der Liste **Zielgeräte** hinzuzufügen. Falls diese Schaltfläche nicht zu sehen ist, klicken Sie auf **<<**.

Wenn mehrere Geräte gefunden wurden, wählen Sie diejenigen aus, die Sie der Liste hinzufügen möchten, und klicken Sie dann auf **Ziel**. Wenn sich die zurückgegebene Geräteliste über mehrere Seiten erstreckt, klicken Sie für jede Seite auf **Ziel**. Es ist nicht möglich, auf mehreren Seiten Geräte auszuwählen und dann nur ein Mal für alle Seiten auf die Schaltflächen zu klicken. Sie können auf den nach unten zeigenden Pfeil unterhalb der Symbolleiste auf der äußersten rechten Seite klicken, um festzulegen, wie viele Geräte Sie pro Seite anzeigen möchten. Sie können bis zu 500 Geräte pro Seite anzeigen. Wie Sie die Anzahl der in der Liste angezeigten Geräte ändern können, erfahren Sie im Abschnitt Seiteneinstellungen unter **Einstellungen**.

Wenn mindestens ein Gerät in der Liste **Zielgeräte** enthalten ist, können Sie einen Task wie das Bereitstellen einer Agentenkonfiguration auf jedem der Zielgeräte durchführen, oder Sie können nicht verwaltete Geräte in die Liste **Eigene Geräte** verschieben.

So bestimmen Sie Zielgeräte

1. Klicken Sie in der Liste **Eigene Geräte** oder in der Ansicht **Erkannte Geräte** auf das Gerät, das Sie als Ziel für eine Aktion auswählen möchten. Mit den Methoden, die standardmäßig für die Auswahl mehrerer Elemente verwendet werden (UMSCHALT+Mausklick oder STRG+Mausklick), können Sie nach Bedarf mehrere Geräte gleichzeitig auswählen.
2. Klicken Sie auf die Schaltfläche **Ziel**. Falls diese Schaltfläche nicht zu sehen ist, klicken Sie in der Symbolleiste auf **<<**. Die Schaltfläche befindet sich ganz rechts.

Die ausgewählten Geräte werden im unteren Fensterbereich unter der Registerkarte **Zielgeräte** aufgelistet. Sobald die Geräte unter dieser Liste aufgelistet werden, können Sie ein Tool öffnen (beispielsweise die Agentenbereitstellung) und einen Task zeitlich planen, der auf die Zielgeräte angewendet werden kann. Wenn Sie nicht verwaltete Geräte als Ziel ausgewählt haben, können Sie auf die Registerkarte **Verwalten** klicken und die Geräte in die Liste **Eigene Geräte** verschieben.

Filtern der Anzeigeliste

Die Liste **Eigene Geräte** verfügt über ein Filtersymbol, mit dem Sie festlegen können, welche Geräte in der Liste angezeigt werden. Sie können die Liste entweder nach nur einem Kriterium (Gerätename oder IP-Adresse) filtern, oder Sie können die Kriterien miteinander kombinieren, um den Fokus auf eine Teilgruppe von Computern zu richten.

So filtern Sie die Anzeigeliste

1. Doppelklicken Sie in der Liste **EigeneGeräte** auf **Alle Geräte** oder navigieren Sie zu einer Gruppe.
2. Klicken Sie auf **Filter** in der Symbolleiste.
3. Wählen Sie in der Dropdown-Liste **Gerätename** oder **IP-Adresse** aus.

4. Setzen Sie die Parameter für die angegebenen Kriterien, indem Sie die entsprechenden Daten in das Textfeld eingeben. Folgende Zeichen des erweiterten Zeichensatzes werden im Feld **Suchen** nicht unterstützt: < , > , " , ' , !.

   Wenn Sie "Nach Gerätename" filtern, geben Sie den Hostnamen oder den Computernamen-Bereich ein. Bei der Suche nach Computernamen können Sie Platzhalter verwenden (z.B. *srv).

5. Klicken Sie auf **Suchen**.

Verwenden von Gruppen

Zur Vereinfachung des Verwaltungsaufwands können Sie Geräte in Gruppen zusammenfassen. Sie können Gruppen erstellen, um Geräte nach Funktion, Standort, Abteilung, Geräteattribut oder einer anderen Kategorie zu ordnen, die Ihren Anforderungen entspricht. Sie können z.B. eine Webserver-Gruppe für alle als Webserver konfigurierten Server erstellen oder alle Geräte, die ein bestimmtes Betriebssystem ausführen, zu einer Gruppe zusammenfassen. Sie können mit der rechten Maustaste auf eine Gruppe klicken, um sie zu öffnen, zu löschen oder alle darin enthaltenen Geräte als Ziel für Aktionen wie Bereitstellung von Alarmregelsätzen und Agenten auswählen.

Die Hauptansicht des Fensters **Eigene Geräte** enthält die folgenden Gruppen:

- **Alle Geräte:** Erstellt eine einfache Liste (keine Untergruppen) mit allen Geräten, die für den zurzeit angemeldeten Benutzer (abhängig von dessen Bereich) sichtbar sind. Für einen Administrator führt **Alle Geräte** alle Geräte auf, die in die Core-Datenbank gescannt oder dorthin verschoben wurden. Mit dem Standard Management Agent konfigurierte Geräte werden automatisch in der Gruppe/dem Ordner **Alle Geräte** angezeigt, wenn sie mit dem Inventarscanner in die Core-Datenbank gescannt werden. Benutzer, einschließlich Administratoren, können keine Gruppen unter **Alle Geräte** erstellen.
- **Öffentliche Gruppen:** Listet Gruppen/Geräte auf, die ein Administrator aus der Gruppe **Alle Geräte** hinzugefügt hat; außerdem werden auch Blade-Gehäuse-Gruppen aufgelistet. Ein Administrator (ein Benutzer mit dem Recht "Administrator") kann alle Geräte in dieser Gruppe anzeigen, während andere Benutzer nur die Geräte sehen können, die zu ihrem Bereich gehören. Nur Administratoren können Gruppen unter **Öffentliche Gruppen** erstellen.
- **Private Gruppen:** Führt die Gruppen/Geräte für die aktuell angemeldeten Benutzer auf, basierend auf dem Benutzerbereich. Der Benutzer kann Geräte-Untergruppen nur unter **Private Gruppen** erstellen. Benutzer können Geräte ihren **Privaten Gruppen** oder einer ihrer Untergruppen hinzufügen, indem sie Server aus den **Öffentlichen Gruppen** und der Gruppe **Alle Geräte** verschieben oder kopieren. Alle Benutzer können Gruppen unter **Private Gruppen** erstellen.

Wenn Sie sich genauer informieren möchten, welche Geräte Sie in der Geräteansicht anzeigen und verwalten und welche Verwaltungstools Sie verwenden können, lesen Sie die Ausführungen unter Rollenbasierte Administration.

Gruppentypen

Sie können zwei verschiedene Gruppentypen erstellen und verwalten:

- **Statische Gruppen**. Eine *statische Gruppe* besteht aus Geräten, die Sie manuell zu der betreffenden Gruppe hinzugefügt haben. Statische Gruppen lassen sich nur durch manuelles Hinzufügen oder Entfernen von Geräten ändern.
- **Dynamische Gruppen**. Eine *dynamische Gruppe* besteht aus Computern, die Filter- oder Abfragekriterien erfüllen. Jedes Mal, wenn die Gruppe erweitert wird, wird die Abfrage aktiviert und das Ergebnis angezeigt. Beispiel: Eine dynamische Gruppe kann alle Geräte beinhalten, die sich gegenwärtig in einem Warnzustand befinden. Mit dem sich ändernden Status der Rechner würden die Rechner in die Gruppe verschoben bzw. aus der Gruppe entfernt.

So erstellen Sie eine statische Gruppe

1. Doppelklicken Sie in der Geräteansicht der Konsole auf die übergeordnete Gruppe (z.B. **Private Gruppen**) und klicken Sie dann auf **Gruppe hinzufügen**.
2. Geben Sie einen Namen für die neue Gruppe ein.
3. Klicken Sie auf **Statisch** und klicken Sie dann auf **OK**.

Nachdem Sie eine statische Gruppe erstellt haben, können Sie Geräte in die Gruppe verschieben oder kopieren, indem Sie sie aus einer Liste auswählen und dann auf **Verschieben/Kopieren** in der Symbolleiste klicken. Sie können Geräte aus der Liste **Alle Geräte** in eine Gruppe kopieren oder aus anderen Gruppen verschieben/kopieren.

So erstellen Sie eine dynamische Gruppe

1. Doppelklicken Sie in der Geräteansicht der Konsole auf die übergeordnete Gruppe (z.B. **Private Gruppen**) und klicken Sie dann auf **Gruppe hinzufügen**.
2. Geben Sie einen Namen für die neue Gruppe ein.
3. Klicken Sie auf **Dynamisch** und klicken Sie dann auf **OK**.

Nachdem Sie eine dynamische Gruppe erstellt haben, müssen Sie einen Filter für die Gruppe definieren, um zu bestimmen, welche Computer in der Gruppe angezeigt werden. Sie können einen neuen Filter erstellen oder eine vorhandene Abfrage als Basis für den Filter verwenden.

So erstellen Sie einen neuen Filter

1. Wählen Sie die von Ihnen erstellte dynamische Gruppe aus (im unteren Fensterausschnitt werden die **Gruppeneigenschaften** angezeigt)
2. Wählen Sie unter **Gruppeneigenschaften** die Option **Neuen Filter erstellen** aus und klicken Sie auf **Neuer Filter**.
3. Wählen Sie die zu verwendenden Filterkriterien aus und klicken Sie auf **OK**.

So erstellen Sie einen Filter, der auf einer vorhandenen Abfrage basiert

1. Wählen Sie die von Ihnen erstellte dynamische Gruppe aus (im unteren Fensterausschnitt werden die **Gruppeneigenschaften** angezeigt)

2. Wählen Sie in den **Gruppeneigenschaften** die Option **Einen Filter erstellen, der auf einer vorhandenen Abfrage basiert** aus.
3. Wählen Sie die vorhandenen Abfrage aus, die Sie zum Filtern der Gruppe verwenden möchten, und klicken Sie auf **Neuer Filter**.
4. Fügen Sie nach Bedarf zusätzliche Filterkriterien hinzu und klicken Sie auf **OK**.

Wenn Sie als Basis für einen Filter eine vorhandene Abfrage wählen und diese Abfrage später von Ihnen oder einem anderen Benutzer modifiziert wird, wird der Filter, der auf dieser Abfrage basiert, nicht automatisch an die geänderte Abfrage angepasst.

Verwenden der Registerkarte "Aktionen"

Verwenden Sie die Registerkarte **Aktionen**, um ausgewählte Server und Zielgeräte mit Aktionen zu bearbeiten. Sie können von dieser Registerkarte aus Geräte aus der Liste der verwalteten Computer löschen, Geräte ein-/ausschalten sowie neu starten und Verbindungen mit verwalteten Geräten überwachen.

- Geräte löschen
- Stromoptionen
- Geräteüberwachung

Geräte löschen

Mit der Funktion **Geräte löschen** können Sie ausgewählte Geräte oder Zielgeräte aus der Liste mit den verwalteten Computern löschen. Die Löschfunktion kann einzelne oder mehrere Geräte aus einer System Manager-Gruppe (entweder einer Standardgruppe oder einer benutzerdefinierten Gruppe) löschen. Nachdem Sie ein Gerät aus einer Gruppe gelöscht haben, wird es aus allen Listen mit verwalteten/inventarisierten Geräten, einschließlich der Standardgruppe **Alle Geräte**, entfernt.

Wenn Sie eine große Anzahl von Geräten löschen, wird die Operation möglicherweise aufgrund einer Zeitüberschreitung abgebrochen. Wenn dies der Fall ist, sollten Sie versuchen, die Operation in mehrere kleinere Vorgänge aufzuteilen.

Stromoptionen

Mit den **Stromoptionen** können Sie Remote-Geräte abschalten, neu starten und (bei verwalteten IPMI-Rechnern) einschalten. Bei Nicht-IPMI-Servern muss auf dem Gerät der LANDesk Agent vorhanden sein, damit die Neustart- und Abschaltfunktionen ausgeführt werden können. Bei IPMI-Rechnern müssen Sie über die korrekten IPMI-Anmeldeinformationen verfügen, um die Einschalt-/Abschalt- und Neustartfunktionen ausführen zu können. Wenn auf einer IPMI-Box der LANDesk Agent bereitgestellt wurde, können Sie die Abschalt- und Neustartfunktionen ohne die IPMI-Anmeldeinformationen ausführen. Verwenden Sie das Dienstprogramm Dienste konfigurieren, um das für die Verwaltung von IPMI-Servern zu verwendende IPMI BMC-Kennwort zu definieren.

So verwenden Sie Stromoptionen

1. Klicken Sie in der Liste **Eigene Geräte** auf ein Gerät oder wählen Sie eine Geräteliste als Ziel aus.
2. Klicken Sie im unteren Fensterausschnitt auf die Registerkarte **Aktionen**.
3. Klicken Sie auf **Stromoptionen**.
4. Wählen Sie, ob die Aktion auf Geräten in der Liste Zielgeräte oder nur auf ausgewählten Geräten ausgeführt werden soll.
5. Wählen Sie eine der folgenden Optionen aus:
   - Neustart
   - Ausschalten
   - Einschalten (funktioniert bei IPMI- und Wake on LAN-fähigen Geräten)

6. Klicken Sie auf **Umleitungsfenster der Konsole anzeigen**, um einen Ultraslim-Container mit einem Launcher zu starten (der Launcher lässt sich für EM64T bedeutend einfacher rekompilieren als das TTY Control).

   Beim Einschalten oder Neustarten eines verwalteten IPMI-Servers können Sie ein Konsolenumleitungsfenster öffnen, in dem die Bootinformationen des Servers angezeigt werden. Dies kann nützlich sein, wenn Sie sicherstellen möchten, dass der Server einen Neustart durchführt. Sie können das Konsolenfenster auch zum Anhalten des Bootprozesses und Ändern von BIOS-Einstellungen auf dem verwalteten Server verwenden.

   Um das Konsolenumleitungsfenster anzuzeigen, muss im BIOS-Setup des Servers die Option "Konsolenumleitung über seriellen Anschluss" (Console redirection over serial port) aktiviert sein. Die Konsolendaten werden an den seriellen Anschluss gesendet. Wenn Server und Administratorkonsole über ein serielles Kabel miteinander verbunden sind, wird die Konsolenumleitung über dieses Kabel realisiert. Falls nicht, initiiert System Manager eine Serial over LAN (SOL)-Verbindung, um die Daten vom seriellen Anschluss zur LAN-Verbindung umzuleiten. Die SOL-Verbindung bleibt geöffnet, solange das Konsolenfenster geöffnet ist. Nachdem alle Konsolendaten angezeigt wurden, sollten Sie das Fenster schließen.

   Beim Öffnen des Konsolenfensters wird ein zweites Meldungsfenster geöffnet. Sie können das Meldungsfenster schließen. Nachdem das Konsolenumleitungsfenster geöffnet wurde (jedoch bevor die Konsole die Bootsequenz anzeigt), werden u.U. arbiträre Zeichen im Fenster angezeigt. Diese Zeichen werden eingeblendet, weil der BMC des Servers Heartbeat-Meldungen sendet, die über die Verbindung an die Administratorkonsole weitergeleitet werden. Die Zeichen sind während der Darstellung der Bootanzeige durch die Konsole nicht zu sehen, sie werden jedoch nach Abschluss des Bootprozesses u. U. erneut eingeblendet.

Geräteüberwachung

Mit der Geräteüberwachung können Sie die Konnektivität der ausgewählten Geräte überwachen. Wenn die Netzwerkverbindung mit einem Gerät getrennt wird, kann der Server keinen Alarm an den Core Server senden. Die Geräteüberwachung prüft nach, ob die Geräte immer noch mit dem Netzwerk verbunden sind.

1. Klicken Sie in der Liste **Alle Geräte** auf ein Gerät oder wählen Sie eine Geräteliste als Ziel aus.
2. Klicken Sie im unteren Fensterausschnitt auf die Registerkarte **Aktionen** und klicken Sie dann auf **Geräteüberwachung**.
3. Zum Anzeigen einer Liste mit gegenwärtig überwachten Geräten klicken Sie auf **Überwachte Geräte anzeigen**.
4. Geben Sie das Minutenintervall zwischen den Ping-Durchläufen an und legen Sie fest, wie oft das Produkt versuchen wird, mit einem Gerät zu kommunizieren.
5. Wählen Sie aus, ob die Aktion auf Geräten in der Liste "Zielgeräte" oder auf allen Geräten in der Gruppe **Alle Geräte** ausgeführt werden soll.
6. Wählen Sie **Nie einen Ping-Test mit dem Gerät durchführen** aus, um die Überwachung einzustellen.
7. Klicken Sie auf **Übernehmen**.

Nur die letzte Gruppe mit Zielgeräten wird überwacht. Wenn Sie z. B. Gerät A und Gerät B als Ziel auswählen und die Geräteüberwachung auf diese Geräte anwenden, werden nur Gerät A und Gerät B vom Core Server einem Ping-Test unterzogen. Wenn Sie anschließend Gerät C und Gerät D als Zielgeräte auswählen und die Geräteüberwachung auf diese Geräte anwenden, werden nur Gerät C und Gerät D überwacht, nicht mehr A und B.

Benutzerdefinierte Spalten

Verwenden Sie die Option **Benutzerdefinierte Spalten** zum Ändern von Spaltennamen und Feldern. Mit Name ist der Name der Spalte gemeint und ein Feld entspricht dem/den Attribut(en), die in der Spalte erscheinen können (sofern das Attribut präsent ist). Alle etwaigen Spaltenänderungen, die Sie vornehmen, sind für den Benutzer unsichtbar. Benutzerdefinierte Spaltenänderungen werden in der Ansicht **Eigene Geräte** angezeigt.

Dieses Produkt enthält einen Standardspaltensatz mit sieben Spalten. Der Standardsatz lässt sich zwar nicht bearbeiten, Sie können jedoch einen benutzerdefinierten Spaltensatz als Ihren Standard-Spaltensatz verwenden.

Es ist nicht zweckmäßig, benutzerdefinierte Spalten zu erstellen, die mehrere Feldnamen unterstützen. Beispiel: Wenn Sie ein "Computer.Software.Package.Name"-Feld erstellen und auf dem Gerät mehrere Pakete installiert sind, listetSystem Manager nur einen Paketnamen pro Zeile auf, selbst dann, wenn sich die anderen Paketnamen auf demselben Gerät befinden; dies führt dazu, dass die Liste **Alle Geräte** mehrere Einträge für dasselbe Gerät anzeigen.

So erstellen Sie einen benutzerdefinierten Spaltensatz

1. Klicken Sie im linken Navigationsfenster auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Benutzerdefinierte Spalten**.
3. Klicken Sie auf **Neu**.
4. Geben Sie einen Namen für den Spaltensatz ein.

5. Wählen Sie im oberen Feld jede Spaltenüberschrift einzeln aus, die Sie im Spaltensatz verwenden möchten und klicken Sie dann auf **Hinzufügen**.

   Das Feld zeigt eine Liste an, die dem gesamten Inventardatenbestand entspricht, der gegenwärtig in der Datenbank enthalten ist. Führen Sie einen Drilldown auf dieser Liste durch, um ein Attribut auszuwählen, das in der Abfrageergebnisliste angezeigt werden soll. Wählen Sie dabei Attribute aus, mit denen Sie die in der Abfrage zurückgegebenen Clients identifizieren können. Wenn Sie keine Attribute finden, die Sie anzeigen möchten, können Sie sie im Dialogfeld Benutzerdefinierte Attribute hinzufügen. Diese Attribute müssen jedoch Computern zugewiesen werden, bevor sie im Abfragedialogfeld angezeigt werden.

   Hinweis: Wenn Sie ein Attribut in der Datenbank auswählen, das über eine 1:*-Beziehung verfügt, erhalten Sie Doppeleinträge für dieses Gerät. Wenn Sie Attribute mit einer 1:1-Beziehung auswählen (nur ein mögliches Attribut, z. B. Computer.System.Asset Tag), erhalten Sie keine Doppeleinträge.

6. Um die Spaltenanordnung zu ändern, wählen Sie eine Spaltenüberschrift aus und klicken auf **Nach oben** oder **Nach unten**.
7. Um eine Spalte zu entfernen, wählen Sie sie aus und klicken auf **Entfernen**.
8. Um die für eine Spalte angezeigte Überschrift zu ändern, wählen Sie die Überschrift im unteren Feld aus, klicken auf **Bearbeiten**, führen die gewünschten Änderungen aus und betätigen die **Eingabetaste**. Die folgenden Zeichen des erweiterten Zeichensatzes werden nicht unterstützt: < , > , ' , " , !.
9. Klicken Sie auf **OK**, um den Spaltensatz zu speichern.
10. Um beim Anzeigen der Liste **Alle Geräte** den benutzerdefinierten Spaltensatz zu verwenden, wählen Sie ihn aus und klicken in der Symbolleiste auf **Als aktuellen Spaltensatz festlegen**.

So bearbeiten Sie einen benutzerdefinierten Spaltensatz

1. Klicken Sie im linken Navigationsfenster auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Benutzerdefinierte Spalten**.
3. Wählen Sie den benutzerdefinierten Spaltensatz aus und klicken Sie auf **Bearbeiten**.
4. Wählen Sie im oberen Feld eine Spaltenüberschrift aus und klicken Sie auf **Hinzufügen**, um ihn der Spalte hinzuzufügen (siehe Hinweise unter Schritt 5 oben).
5. Um eine Spalte zu entfernen, wählen Sie sie aus und klicken auf **Entfernen**.
6. Um die für eine Spalte angezeigte Überschrift zu ändern, wählen Sie die Überschrift im unteren Feld aus, klicken auf **Bearbeiten**, führen die gewünschten Änderungen aus und betätigen die **Eingabetaste**. Die folgenden Zeichen des erweiterten Zeichensatzes werden nicht unterstützt: < , > , ' , " , !.
7. Um die Spaltenanordnung zu ändern, wählen Sie eine Spaltenüberschrift aus und klicken auf **Nach oben** oder **Nach unten**.
8. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Benutzerdefinierte Attribute

Attribute sind Merkmale oder Eigenschaften, die mit einem Gerät verknüpft sind. Je mehr Attribute ein Gerät in der Datenbank besitzt, umso einfacher ist es, das Gerät eindeutig zu identifizieren. Benutzerdefinierte Attribute können von Ihnen nur erstellt werden, wenn Sie LANDesk® Server Manager mit dem Administratorrecht verwenden. Wenn benutzerdefinierte

Attribute erstellt und der Core-Datenbank hinzugefügt wurden, können Sie einem verwalteten Gerät Werte für diese Attribute zuweisen. Wenn der Core-Datenbank keine benutzerdefinierten Attribute hinzugefügt wurden, wird die Option **Attribute zuweisen** auf der Registerkarte **Aktionen** nicht angezeigt.

So weisen Sie Geräten benutzerdefinierte Attribute zu

1. Wählen Sie in der Liste **Alle Geräte** mindestens ein Gerät aus.
2. Klicken Sie im unteren Fensterausschnitt auf die Registerkarte **Aktionen**.
3. Wählen Sie im linken Fensterausschnitt **Attribute zuweisen**.
4. Zu jedem Attributnamen gehört eine Dropdown-Liste mit Werten. Wählen Sie für den Attributnamen einen Wert aus der Dropdown-Liste aus und wiederholen Sie den Vorgang nach Bedarf. Klicken Sie auf **Ausgewählte Geräte**.
5. Klicken Sie auf **Zuweisen** und klicken Sie dann auf **OK**.

Sie können auch benutzerdefinierte Attribute mehreren Zielgeräten zuweisen. Wenn in der Liste "Ziel" Geräte enthalten sind, klicken Sie in Schritt 4 oben auf **Zielgeräte**.

Seiteneinstellungen

Verwenden Sie die Seite **Seiteneinstellungen** zum Festlegen des Anzeigelayouts von Seiten, auf denen Geräte aufgelistet oder Grafiken angezeigt werden.

1. Klicken Sie im linken Navigationsfenster auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Seiteneinstellungen**.
3. Wählen Sie in der Dropdown-Liste **Diagrammtyp** den Diagrammtyp aus, den Sie unter **Berichte** anzeigen möchten.
4. Geben Sie in das Feld **Elemente/Seite** die maximale Anzahl von Elementen ein, die Sie auf den Seiten, die Paginierung verwenden, jeweils anzeigen möchten. Der maximal zulässige Wert ist 500.

Einsteigermodus

Sie können entlang der Schaltflächen auf den Symbolleisten Text einblenden, um neuen Benutzern die Verwendung der Funktionen zu erleichtern. Wenn diese Option nicht ausgewählt ist, werden nur Symbole auf den Symbolleisten angezeigt. Für die Symbole wird Text eingeblendet, wenn Sie mit der Maus auf die Symbole zeigen.

1. Um entlang der Schaltflächen auf den Symbolleisten Text anzuzeigen, aktivieren Sie das Kontrollkästchen**Text auf Symbolleisten anzeigen**.
2. Klicken Sie auf **Aktualisieren**.

Anzeigen der Serverinformationskonsole

Mit der Serverinformationskonsole können Sie Übersichtsdaten zu einem Gerät sowie Systeminformationen wie CPU- oder Lüfterdaten anzeigen, den Serverzustand und Grenzwerte wichtiger Gerätebestandteile überwachen, Anfälligkeiten verwalten sowie ein Gerät ein- oder

abschalten und neu starten. Im linken Navigationsfenster der Serverinformationskonsole befinden sich folgende Abschnitte:

- Systeminformationen
- Software-Updates
- Überwachung
- Regelsätze
- Stromoptionen
- Hardware-Konfiguration

Um die Serverinformationskonsole für ein Gerät anzeigen zu können, muss zuerst der Standard Management Agent auf diesem Gerät installiert werden (siehe Konfigurieren von Agenten). Außerdem muss das Gerät nach Installation des Agenten neu gestartet werden, damit die Serverinformationskonsole richtig funktioniert. Ein Neustart ist bei Installation von Agenten sowohl auf dem Core Server als auch auf verwalteten Geräten erforderlich.

So zeigen Sie die Serverinformationskonsole an

1. Doppelklicken Sie in der Liste **Eigene Geräte** auf den Gerätenamen.

   Die Konsole wird ein einem neuen Browser-Fenster geöffnet. Standardmäßig wird die **Zustandsübersicht** angezeigt.

2. Klicken Sie auf die Schaltflächen im linken Navigationsfensterausschnitt, um die Serverinformationen anzuzeigen und die verfügbaren Tools zu verwenden.

Systeminformationen

Systeminformationen enthält eine Zusammenfassung des Systemzustands sowie Informationen über Hardware und Software, Systemprotokolle und andere Daten wie Informationen zu den vorhandenen Geräten und zum Netzwerk.

Zustand Übersicht

Die Seite **Zustand Übersicht** gibt eine schnelle Übersicht über den Systemzustand des jeweiligen Geräts. Sie erkennen auf einen Blick, ob die ausgewählten Hardwareelemente wie vorgesehen funktionieren und ob sich Probleme abzeichnen, denen Sie ggf. Aufmerksamkeit schenken müssen.

Wenn sich einer der Systemfaktoren in einem Warn- oder kritischen Zustand befindet, wird in der zugehörigen Schaltfläche ein gelbes (Warnung) oder rotes (kritisch) Symbol eingeblendet, das auf das Problem hinweist. Klicken Sie auf die Schaltfläche, um eine Beschreibung des auslösenden Ereignisses anzuzeigen.

System Übersicht

Verwenden Sie die Seite **System Übersicht**, um wichtige Informationen zum ausgewählten Gerät anzuzeigen. Die angegebenen Informationen können Folgendes umfassen, je nach Hardware- und Softwarekonfiguration des Geräts:

- **Zustand:** Der Gesamtzustand des Geräts gemäß den von Ihnen festgelegten Bedingungen und Parameter.
- **Typ:** Der Gerätetyp, beispielsweise Druck-, Programm- oder Datenbankserver.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Das Gerätemodell.
- **BIOS-Version:** Die BIOS-Version des Geräts.
- **Betriebssystem:** Das Betriebssystem des Geräts.
- **Betriebssystemversion:** Die Versionsnummer des Betriebssystems.
- **CPU:** Hersteller, Modell und Geschwindigkeit des Geräteprozessors.
- **Anfälligkeitsscanner:** Die Version des Anfälligkeitsscanners.
- **Fernsteuerung:** Die Version des Fernsteuerungsagenten.
- **Softwareverteilung:** Die Version des Softwareverteilungsagenten.
- **Inventarscanner:** Die Version des Inventarscanners.
- **IPMI-Typ, IPMI-Version:** Die vom Gerät verwendete IPMI-Version und IPMI-Typ.
- **SDR-Version:**Die Version des Sensordatensatzes im BMC des Geräts.
- **BMC-Version:** Die Version des Baseboard Management Controllers auf dem Gerät.
- **Kern:** Bei Linux-Geräten die Versionsnummer des installierten Kerns.
- **Überwachung:** Die Versionsnummer des Überwachungsagenten auf dem Gerät.
- **CPU-Nutzung:** Prozentsatz des derzeit verwendeten Prozessors.
- **Physikalischer Speicher verwendet*:** Der Prozentsatz des insgesamt auf dem Gerät verwendeten physikalischen Speichers.
- **Virtueller Speicher verwendet*:** Der Prozentsatz des insgesamt auf dem Gerät verwendeten virtuellen Speichers.
- **Letzter Neustart*:** Datum und Uhrzeit des letzten Geräte-Neustarts (in der Zeitzone der Datenbank).
- **Laufwerk:** Die Laufwerke auf dem Gerät unter Angabe der Gesamtgröße des Laufwerks und des Prozentsatzes an verwendetem Speicher.

Diese Informationen werden aus der Registrierung in Windows oder aus den Konfigurationsdateien in Linux abgerufen.

*Diese Informationen werden angezeigt, wenn ein Agent auf dem Gerät installiert ist.

Hardware

Verwenden Sie die Seite **Hardware**, um Details zur Hardware-Konfiguration des Geräts anzuzeigen. Die Einträge in der Liste **Hardware** sind nach folgenden Kategorien gruppiert. Nicht alle Kategorien werden für alle Geräte angezeigt. Wenn das Gerät z. B. keinen Lüfter und keine Temperatursensoren hat, erscheint die Kategorie **Kühlung** nicht in dieser Liste.

- **CPU:** Prozessoren und Cache
- **Speicher:** logische Laufwerke, physikalische Laufwerke, mobile Medien und Speicheradapter

- **Speicher:** Speichernutzung und Speichermodule
- **Gehäuse:** das Gehäuse des Servers; Anzeige, ob das Gehäuse offen oder geschlossen ist
- **Eingabegeräte:** Tastatur, Maus und andere Geräte
- **Motherboard:** Motherboard, Steckplätze und BIOS
- **Kühlung:** Lüfter und Temperatursensoren
- **Strom:** Netzgeräte und Spannung

Einstellen von Warngrenzwerten für Hardware-Komponenten

Einige Komponenten in der Liste **Hardware** enthalten Daten von Sensoren im Gerät, wie z. B. Temperatursensoren. Wenn ein verwaltetes Gerät über Komponenten mit unterstützten Sensoren verfügt, können Sie die Sensormesswerte ändern, die einen Alarm auslösen. So kann z. B. für den CPU-Temperatursensor bei Unter- bzw. Überschreitung bestimmter Messwerte eine Warnmeldung oder kritischer Alarm ausgelöst werden. Die Grenzwerte richten sich in der Regel nach den vom Hersteller empfohlenen Einstellungen, Sie können jedoch die oberen und unteren Grenzwerte im Dialogfeld **Grenzwerte** ändern.

1. Klicken Sie in der Serverinformationskonsole auf **Systeminformationen**.
2. Erweitern Sie den Ordner **Hardware** und suchen Sie das gewünschte Hardware-Element in den Unterordnern (z. B. **Kühlung | Temperaturen**).
3. Doppelklicken Sie in der Liste der Sensoren auf den Sensor, dessen Grenzwerte Sie ändern möchten.
4. Geben Sie die gewünschten Werte in die Textfelder für den unteren und/oder oberen Grenzwert ein oder ziehen Sie die Schieberegler auf dem Trackbar nach links oder rechts, um die Werte zu ändern.
5. Klicken Sie auf **Update**, um Ihre Änderungen zu speichern.
6. Klicken Sie zum Wiederherstellen der ursprünglichen Grenzwerte auf **Standardeinstellungen wiederherstellen**.

Protokolle

Die Seite "Protokolle" zeigt die lokalen Systemprotokolle, das System Events Log (SEL) für IPMI-Geräte und ein Alarmprotokoll an.

Lokale Protokolle wie die Anwendungs-, Sicherheits- und Systemprotokolle besitzen keine Schaltfläche, mit der sich das Protokoll auf der Konsole löschen lässt; Sie können die Protokolle jedoch mithilfe des Windows Computer Management anzeigen und löschen.

Wenn das BIOS über die Funktionalität zum Löschen des SMBIOS-Protokolls verfügt, klicken Sie auf die Schaltfläche **Protokoll löschen**, um alle Protokolleinträge zu entfernen. Diese Schaltfläche ist nicht verfügbar, wenn dieser Vorgang vom BIOS nicht unterstützt wird.

Software

Die Seite **Software** zeigt zusammenfassende Informationen über Prozesse, Dienste und Pakete auf dem jeweiligen Gerät an sowie eine Liste der aktuellen Umgebungsvariablen.

- **Prozesse:** zeigt die laufenden Prozesse an; wählen Sie einen Prozess aus und klicken Sie auf **Prozess beenden**, um ihn zu beenden
- **Dienste:** zeigt die auf dem Gerät verfügbaren Dienste sowie deren Status an; wählen Sie einen Dienst aus und klicken Sie auf **Stopp**, **Start** oder **Neu starten**, um Änderungen vorzunehmen.
- **Pakete:** gibt die installierten Pakete mit Versionsnummern und Namen der Lieferanten an.
- **Umgebung:** gibt die derzeit für das Gerät eingestellten Umgebungsvariablen an.

Sonstige

Die Seite **Sonstige** enthält Inventarinformationen sowie eine Zusammenfassung der Netzwerk-Hardware und -Verbindungen.

- **Inventarinformationen:** zeigen Sie Inventarverwaltungsinformationen, wie z. B. Standort und Inventarkennzeichen-Nummer, an und bearbeiten Sie sie. Außerdem können Sie Systeminformationen wie Seriennummer, Hersteller und Gehäuseart anzeigen.
- **Netzwerkinformation:** Anzeige einer Liste der installierten Netzwerk-Hardware, der Statistiken für die Netzwerkaktivität, einer Konfigurationsübersicht (einschließlich IP-Adresse, Standard-Gateway-Adresse sowie WINS-, DHCP- und DNS-Serverinformationen) und einer Liste der aktuellen Netzwerkverbindungen (zugeordnete Laufwerke)

Software-Updates

Verwenden Sie die Seite **Software-Updates**, um das ausgewählte Gerät auf Anfälligkeiten zu scannen.

So überprüfen Sie erkannte Anfälligkeiten

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem neuen Browser-Fenster wird die Serverinformationskonsole geöffnet.

2. Klicken Sie im linken Navigationsfenster auf **Software-Updates**.

Spaltenbeschreibungen

- **Kennung:** Gibt den eindeutigen, vom Anbieter definierten alphanumerischen Code der Anfälligkeit an.
- **Schweregrad:** Gibt den Schweregrad der Anfälligkeit an. Mögliche Schweregrade sind: "Service Pack", "Kritisch", "Hoch", "Mittel", "Niedrig", "Nicht anwendbar" und "Unbekannt".
- **Titel:** Kurze Beschreibung des Anfälligkeitstyps und -ziels.
- **Sprache:** Gibt die Sprache des Betriebssystems an, die von der Anfälligkeit betroffen ist.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem die Anfälligkeit vom Anbieter veröffentlicht wurde.
- **Unbeaufsichtigte Installation:** Gibt an, ob die mit der Anfälligkeit verknüpfte Patch-Datei unbeaufsichtigt (ohne Benutzerbeteiligung) installiert wird. Einige Anfälligkeiten können mit mehreren Patches verknüpft sein. Wenn eines der Patches einer Anfälligkeit sich nicht unbeaufsichtigt installieren lässt, ist das Attribut **Unbeaufsichtigte Installation** auf **Nein** festgelegt.

- **Reparierbar:** Gibt an, ob sich die Anfälligkeit durch Bereitstellung und Installation einer Patch-Datei reparieren lässt. Zu den möglichen Werten gehören: "Ja", "Nein", "Einige" (für eine Anfälligkeit, die mehrere Erkennungsregeln einschließt, und wenn nicht alle erkannten Anfälligkeiten repariert werden können).

Überwachung

Verwenden Sie die **Überwachung** zur Anzeige von Leistungszählern und Diagrammen und zum Definieren von Grenzwerten für Gerätekomponenten. Nähere Informationen zu dieser Funktion finden Sie im AbschnittGeräteüberwachung.

So wählen Sie einen zu überwachenden Leistungszähler aus

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem neuen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
3. Klicken Sie auf die Registerkarte **Einstellungen für die Leistungszähler**.
4. Wählen Sie in der Spalte **Objekte** das zu überwachende Objekt aus.
5. Wählen Sie in der Spalte **Instanzen** ggf. die Instanz des zu überwachenden Objekts aus.
6. Wählen Sie in der Spalte **Zähler** den zu überwachenden Zähler aus.
7. Geben Sie das Abfrageintervall an und die Anzahl von Tagen, die der Zählerverlauf gespeichert werden soll.
8. Geben Sie im Textfeld **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** an, wie oft der Zähler die Grenzwerte überschreiten darf, ehe ein Alarm generiert wird.
9. Geben Sie die unteren und/oder oberen Grenzwerte an.
10. Klicken Sie auf **Übernehmen**.

So zeigen Sie das Leistungsdiagramm für einen überwachten Zähler an

1. Klicken Sie auf die Registerkarte **Aktive Leistungszähler**.
2. Wählen Sie einen Zähler aus der Liste aus.
3. Wählen Sie in der Dropdown-Liste **Zähler** den Zähler aus, für den Sie ein Leistungsdiagramm anzeigen möchten.
4. Wählen Sie **Echtzeitdaten anzeigen**, um ein Diagramm der derzeitigen Leistung einzublenden. Oder wählen Sie **Vergangenheitsdaten anzeigen** aus, um ein Diagramm einzublenden, das über die Leistung Auskunft gibt, die während des Zeitraums erzielt wurde, den Sie beim Auswählen des Zählers (mit der Option "Verlauf speichern") festgelegt hatten.

Im Leistungsdiagramm repräsentiert die Horizontalachse den verstrichenen Zeitraum. Die Vertikalachse repräsentiert die gemessenen Einheiten, beispielsweise Byte/Sek. (beim Überwachen von Dateiübertragungen), Prozent (beim Überwachen des Prozentsatzes der CPU-Nutzung) oder verfügbare Byte (beim Überwachen des Festplattenspeichers).

Regelsätze

Verwenden Sie die Seite **Regelsätze**, um eine Liste mit den Alarm- und Überwachungsregelsätzen anzuzeigen, die dem ausgewählten Gerät zugewiesen wurden; Sie können mit dieser Seite auch detaillierte Informationen zu den einzelnen Alarmen anzeigen.

So zeigen Sie Alarm-Regelsätze an

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem neuen Browser-Fenster wird die Konsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Regelsätze**.
3. Klicken Sie auf die Registerkarte **Regelsätze für die Alarmierung**.

Der nachstehende Abschnitt beschreibt die Details, die für den jeweiligen Alarm zur Verfügung gestellt werden. Weitere Informationen dazu, wie Sie diese Details ändern können, finden Sie unter Verwenden von Alarmen.

- **Wenn Status erreicht:** Wenn der Status des Alarms den angezeigten Status erreicht, wird ein Alarm ausgelöst.
- **Beeinflusst Zustand:** Wenn der Alarmzustand den angegebenen Grenzwert erreicht, beeinflusst der Zustand den Gesamtzustand des Geräts. Die Auswahl eines den Gesamtzustand beeinflussenden Alarms wird im Dialogfeld "Alarm-Regelsätze" festgelegt.
- **Regelsatz-Name:** Der Name des Alarm-Regelsatzes (entsprechend der Definition im Dialogfeld Alarm-Regelsätze).
- **Alarmtyp:** Der zu generierende Alarmtyp, beispielsweise eine E-Mail, eine SNMP-Trap oder eine Programmausführung.
- **Aktionskonfiguration:** Die Aktion, die abläuft, wenn der Alarm generiert wird (entsprechend der Definition im Dialogfeld Aktion-Regelsätze.
- **Alarm-Handler:** Der mit dem Handler verknüpfte Alarm, beispielsweise ein E-Mail-Handler.
- **Instanz:** Gibt die genaue Quelle des Alarms an.

So zeigen Sie Überwachungsregelsätze an

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem neuen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Regelsätze**.
3. Klicken Sie auf die Registerkarte **Regelsätze für die Überwachung**.

Der nachstehende Abschnitt beschreibt die Details, die für den jeweiligen Überwachungs-Regelsatz zur Verfügung gestellt werden. Weitere Informationen dazu, wie Sie diese Details ändern können, finden Sie unter Informationen zur Überwachung.

- **Name:** Der Name der Regelsatz-Konfiguration (entsprechend der Definition auf der Seite Überwachung).
- **Regelsatz-Name:** Gibt an, ob der Regelsatz ein Standardregelsatz ist oder nicht.
- **Aktiviert:** Der Regelsatz konnte oder konnte nicht auf dem Gerät ausgeführt werden.
- **Grenzwert für die Warnung:** Der Grenzwert, bei dessen Überschreitung das Gerät eine Warnmeldung an den Core sendet.

- **Kritischer Grenzwert:** Der Grenzwert, bei dessen Überschreitung das Gerät eine kritische Meldung an den Core sendet.
- **Überprüfen jeden:** Das Überwachungsintervall für das Element.

Stromoptionen

Mit den **Stromoptionen** können Sie Remote-Geräte abschalten, neu starten und (im Falle verwalteter IPMI und Intel AMT-Geräte) einschalten. Bei Nicht-IPMI-Servern muss auf dem Server der LANDesk Agent vorhanden sein, damit die Neustart- und Abschaltfunktionen ausgeführt werden können.

Bei IPMI- und Intel AMT-Geräten müssen Sie die korrekten Berechtigungsnachweise konfiguriert haben, um die Einschalt-/Abschalt- und Neustartfunktionen ausführen zu können. Wenn auf IPMI- oder Intel AMT-Geräten der LANDesk Agent bereitgestellt wurde, können Sie die Abschalt- und Neustartfunktionen ohne die IPMI- oder Intel AMT-Anmeldeinformationen durchführen. Verwenden Sie zum Konfigurieren von BMC-Anmeldeinformationen für IPMI- oder Intel AMT-Geräte das Dienstprogramm "Dienste konfigurieren" (siehe Konfigurieren von Diensten und Anmeldeinformationen).

So verwenden Sie die Stromoptionen auf dem ausgewählten Gerät

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem neuen Browser-Fenster wird die Konsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Stromoptionen**.
3. Wählen Sie eine der folgenden Optionen aus:
    - Neustart
    - Ausschalten
    - Einschalten

Hardware-Konfiguration

Mit dem Tool **Hardware-Konfiguration** können Sie Optionen für IPMI- oder Intel* AMT-fähige Geräte einstellen. Dieses Tool und die Optionen werden nur bei Geräten angezeigt, die über die entsprechende Hardware verfügen (Beispiel: IPMI-Optionen werden nur angezeigt, wenn das Gerät als IPMI-Gerät erkannt wird).

Sie können Kennungen zur Versorgung von Intel AMT-Geräten generieren, die erstellten Kennungen anzeigen und die Konfigurationsoptionen für die Versorgung Ihrer Intel AMT-Geräte ändern. Außerdem können Sie Leistungsschalterrichtlinien definieren, die verdächtige Netzwerkaktivitäten auf den Geräten erkennen und blockieren, und Sie können die Agentenpräsenzüberwachung aktivieren, um sicherzustellen, dass die Management-Agenten auf Ihren Geräten ständig laufen. (Ausführliche Informationen hierzu finden Sie unter Intel AMT-Support.)

Für IPMI-Geräte können Sie die Konfigurationsoptionen, wie Watchdog-Zeitgeber, Stromoptionen und BMC-Benutzereinstellungen, an Ihre Bedürfnisse anpassen. Außerdem können Sie einen

LAN-Kanal oder eine Serial-Over-LAN-Verbindung konfigurieren, um die Out-of-Band-Kommunikation mit dem IPMI-Gerät aufrecht zu erhalten. (Weitere Informationen finden Sie unter IPMI BMC-Konfiguration.)

Bei Geräten mit einem Dell* DRAC (Remote Access Controller) können Sie die Dell DRAC-Protokolle anzeigen und die Benutzernamen für den Zugang zum OpenManage Server Administrator bearbeiten. (Weitere Informationen finden Sie unter Verwalten von Dell DRAC-Geräten.")

Verwalten von Intel* AMT-Geräten

Nachdem ein Intel* AMT-Gerät erkannt und der Core-Datenbank hinzugefügt wurde (damit es verwaltet werden kann), kann das Gerät in eingeschränktem Umfang verwaltet werden, auch wenn kein LANDesk Agent auf dem Gerät installiert ist. (Weitere Informationen zum Erkennen von Geräten und Verschieben in die Core-Datenbank finden Sie unter Erkennen von Intel* AMT-Geräten.)

In der folgenden Tabelle werden die Verwaltungsoptionen aufgelistet, die einem Gerät zur Verfügung stehen, auf dem nur Intel AMT installiert ist, verglichen mit einem Gerät, das über Intel AMT und einen System Manager Management Agent verfügt.

	Nur Intel AMT	**Intel AMT und Agent**	**Nur Agent**
Inventar	Übersicht	X	X
Ereignisprotokoll	X	X	X
Remote-Boot-Manager	X	X	
Betriebssystemnetzwerk deaktivieren		X	
Betriebssystemnetzwerk aktivieren		X	
Vulscan beim Neustart erzwingen		X	
Inventarverlauf		X	X
Fernsteuerung		X	X

	Nur Intel AMT	Intel AMT und Agent	Nur Agent
Chat		X	X
Dateiübertragung		X	X
Fernausführung		X	X
Reaktivieren		X	X
Herunterfahren		X	X
Neustart		X	X
Inventarscan		X	X
Geplante Tasks und Richtlinien	beschränkt	X	X
Gruppenoptionen		X	X
Inventarbericht ausführen		X	X
Intel AMT-Warnungen		X	X

So zeigen Sie die Intel AMT-Inventarübersicht für ein Gerät an

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie in der Serverinformationskonsole auf **Intel AMT-Optionen**.
3. Klicken Sie auf **Inventarübersicht**.

Die Übersicht enthält Folgendes: GUID-Zahl (GUID, Globally Unique Identifier), Produkt- und Herstellername, Seriennummer, BIOS, Prozessor, Speicherübersichten, Intel AMT-Seriennummer. Falls Informationen fehlen, können Sie die Daten aktualisieren, indem Sie auf **Inventar aktualisieren** klicken.

Zugreifen auf Geräte, die mit dem Enterprise-Modus bereitgestellt wurden

Wenn Sie ein Intel AMT-Gerät im Enterprise-Modus bereitstellen, installiert der Core Server ein Zertifikat für die sichere Kommunikation auf dem Gerät. Wenn das Gerät von einem anderen Core Server verwaltet werden soll, muss die Bereitstellung des Geräts rückgängig gemacht und muss das Gerät dann vom neuen Core Server erneut bereitgestellt werden. Wenn dies nicht geschieht, reagiert der Intel AMT-Zugriff des Geräts nicht, da der neue Core Server kein übereinstimmendes Zertifikat besitzt. Gleichermaßen gilt, dass andere Computer, die versuchen, auf die Intel AMT-Funktionalität zuzugreifen, scheitern werden, da sie kein übereinstimmendes Zertifikat besitzen. (Weitere Informationen zu den Versorgungsmodi finden Sie unter Intel* AMT-Support.)

Intel AMT-Ereignisprotokoll

System Manager stellt eine Ansicht des Ereignisprotokolls bereit, das von den Intel AMT-Geräten generiert wird. Die Einstellungen bestimmen, welche Ereignisse in diesem Protokoll aufgezeichnet werden. Sie können das Datum/die Uhrzeit des Ereignisses, die Quelle des Ereignisses (Einheitsspalte), eine Beschreibung und den durch die Intel AMT-Einstellungen festgelegten Schweregrad (Kritisch oder Nicht-kritisch) anzeigen. Sie können außerdem die Protokolldaten in einem kommabegrenzten (CSV-)Format exportieren.

So zeigen Sie das Intel AMT-Ereignisprotokoll an

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie in der Serverinformationskonsole auf **Systeminformationen**.
3. Erweitern Sie **Protokolle** und klicken Sie auf **Intel AMT-Protokoll**.
4. Um das Protokoll in eine CSV-Datei zu exportieren, klicken Sie auf die Schaltfläche **Exportieren** auf der Symbolleiste und geben den Speicherort an, in dem die Datei gespeichert werden soll.
5. Um alle Daten im Protokoll zu löschen, klicken Sie auf die Schaltfläche **Protokoll entfernen** in der Symbolleiste.
6. Zur Aktualisierung der Protokolleinträge klicken Sie auf die Schaltfläche **Protokoll aktualisieren** in der Symbolleiste.

Intel AMT-Energieoptionen

System Manager enthält Optionen zum Ein- und Ausschalten von Intel AMT-Geräten. Sie können diese Optionen auch dann verwenden, wenn das Betriebssystem eines Geräts nicht reagiert, solange das Gerät mit dem Netzwerk verbunden ist und über Standby-Strom verfügt.

Wenn System Manager Energieoptionsbefehle initiiert, lässt sich in manchen Fällen nicht verifizieren, ob die Befehle auf der Hardware, die den Befehl empfängt, unterstützt werden. Einige Geräte, die über Intel AMT verfügen, unterstützen ggf. nicht alle Energieoptionen (ein Gerät unterstützt möglicherweise IDE-R-Neustarts von einer CD, jedoch nicht von einer Floppy). Informieren Sie sich in der Dokumentation des Hardwareherstellers, wenn Sie den Eindruck haben, dass eine Energieoption auf einem bestimmten Gerät nicht funktioniert. Erkundigen Sie sich bei Intel auch über Firmware- oder BIOS-Aktualisierungen für das Gerät, wenn Energieoptionen nicht wie erwartet funktionsfähig sind.

Sie können einfach die Stromzufuhr des Geräts ein- oder ausschalten, oder Sie können einen Neustart ausführen und bestimmen, wie das Gerät neu gestartet wird. Die Optionen werden in der folgenden Tabelle beschrieben.

Ausschalten	Schaltet die Stromzufuhr zum Gerät aus
Einschalten	Schaltet die Stromzufuhr zum Gerät ein
Neustart	Schaltet den Strom auf dem Gerät aus und dann wieder ein
Normaler Start	Startet das Gerät mit der Startsequenz, die als Standard auf dem Gerät eingestellt ist
Von der lokalen Festplatte starten	Erzwingt einen Start von der Festplatte des Geräts aus, unabhängig vom Standardstartmodus auf dem Gerät
Vom lokalen CD/DVD-Laufwerk starten	Erzwingt einen Start von der CD oder dem DVD-Laufwerk des Geräts aus, unabhängig vom Standardstartmodus auf dem Gerät
PXE-Start	Wenn das PXE-aktivierte Gerät neu gestartet wird, sucht es einen PXE-Server im Netzwerk; wenn einer gefunden wird, wird eine PXE-Startsitzung auf dem Gerät gestartet
IDE-R-Start	Startet das Gerät neu mit der ausgewählten IDE-Umleitungsoption (siehe unten)
BIOS-Setup eingeben	Wenn das Gerät gestartet wird, kann der Benutzer das BIOS-Setup eingeben
Umleitungsfenster der Konsole anzeigen	Wenn das Gerät gestartet wird, wird es im seriellen Modus über dem LAN-Modus gestartet, um ein Konsolenumleitungsfenster anzuzeigen
IDE-Umleitung: Von Diskettenlaufwerk neu starten	Wenn das Gerät gestartet wird, startet es vom Floppy-Laufwerk oder -Abbild aus, das angegeben wurde (Floppy-Abbilddateien müssen

	das Format .img aufweisen, siehe Hinweis)
IDE-Umleitung: Von CD/DVD neu starten	Wenn das Gerät gestartet wird, startet es vom CD-Laufwerk oder -Abbild aus, das angegeben wurde (CD-Abbilddateien müssen das Format .iso aufweisen, siehe Hinweis)
IDE-Umleitung: Von einer angegebenen Abbilddatei neu starten	Wenn das Gerät gestartet wird, wird es von der angegebenen Abbilddatei gestartet (siehe Hinweis weiter unten)

So verwenden Sie die Intel AMT-Energieoptionen

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie in der Serverinformationskonsole auf **Stromoptionen**.
3. Wählen Sie einen Energiebefehl aus. Wenn Sie **Neustart** auswählen, wählen Sie eine Startoption.
4. Klicken Sie auf **Senden**, um den Befehl zu starten.

Hinweise zur Verwendung von IDE-Umleitungsoptionen

Zur Verwendung von IDE-Umleitungsoptionen müssen Sie sowohl eine Startdiskette oder Floppy-Abbilddatei als auch eine Start-CD/-DVD oder CD-/DVD-Abbilddatei angeben. Floppy-Abbilddateien müssen das Format .img und CD-Abbilddateien das Format .iso aufweisen. Einige BIOS erfordern evtl., dass sich das CD-Abbild auf einer Festplatte befindet.

Intel AMT zeichnet im Normalfall die letzten IDE-R-Einstellungen auf; jedoch löscht System Manager die Einstellungen nach 45 Sekunden, sodass die IDE-R-Funktion bei nachfolgenden Startverfahren nicht gestartet wird. Die IDE-R-Sitzung auf einem Intel AMT-Gerät dauert 6 Stunden oder bis die System Manager-Konsole ausgeschaltet wird. Alle IDE-R-Vorgänge, die nach 6 Stunden noch nicht abgeschlossen sind, werden abgebrochen.

Erzwingen eines Anfälligkeitsscans und Deaktivieren des Netzwerkzugriffs auf Intel AMT-Rechnern

Wenn der LANDesk Agent auf einem mit Intel AMT konfigurierten Gerät installiert ist, stellt er Funktionen bereit, die Sie bei der Behebung von Problemen unterstützen können, die durch schädliche Software oder durch andere Probleme, die den Zugriff auf das Gerät verhindern, verursacht wurden.

Der amtmon.exe-Dienst wird mit dem LANDesk Agent installiert. Wenn dieser Dienst auf einem Gerät läuft, können Sie einen Anfälligkeitsscan beim nächsten Neustart erzwingen, um schädliche Software auf dem Gerät zu identifizieren. Falls die Kommunikation mit dem Gerät nicht gelingt, können Sie die Netzwerkverbindung des Geräts deaktivieren, auch wenn das Betriebssystem nicht funktioniert, wie zum Beispiel wenn schädliche Software alle CPU-Zyklen aufgebraucht und dadurch das Betriebssystem deaktiviert hat. Durch Deaktivieren der

Netzwerkverbindung können Sie vermeiden, dass das Gerät unerwünschte Pakete über das Netzwerk versendet.

Wenn der LANDesk Agent auf einem Intel AMT-Gerät installiert ist, werden die folgenden Optionen auf der Seite **Intel AMT-Optionen** bereitgestellt:

- **Betriebssystem-Netzwerkverbindung:** Klicken Sie auf **Deaktivieren**, um den Betriebssystem-Netzwerk-Stack zu deaktivieren, um dadurch den Zugriff auf das Netzwerk zu stoppen; klicken Sie auf **Aktivieren**, um den Betriebssystem-Netzwerkzugriff zu aktivieren, falls er deaktiviert war.
- **Nach dem Neustart nach Anfälligkeiten suchen:** Erzwingt die Ausführung des Anfälligkeitsscanners beim nächsten Neustart des Geräts.

Wenn ein Gerät nicht reagiert oder schädliche Software auf ihm ausgeführt wird, ist es empfehlenswert, beim nächsten Neustart zuerst einen Anfälligkeitsscan auszuführen, um das Problem zu identifizieren. Wenn das Problem weiterhin besteht und der Computer das Netzwerk infiziert/angreift, oder wenn Sie nicht auf das Gerät zugreifen können, haben Sie die Möglichkeit, die OS NIC (Netzwerkschnittstellenkarte des BS) zu deaktivieren.

So erzwingen Sie einen Anfälligkeitsscan nach einem Neustart

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie im Konsolenfenster des Geräts auf **Intel AMT-Optionen**.
3. Klicken Sie auf **Konfigurationsoptionen** und klicken Sie dann auf **Scannen**. Eine Nachricht erscheint auf dem Gerät und meldet, dass beim nächsten Neustart ein Scan ausgeführt wird.
4. Um das Gerät auszuschalten oder neu zu starten, verwenden Sie die oben beschriebenen Funktionen des Intel AMT-Remote-Startmanagers.

So deaktivieren oder aktivieren Sie die Netzwerkverbindung auf einem nicht reagierenden Gerät

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie im Konsolenfenster des Geräts auf **Intel AMT-Optionen**.
3. Um durch Deaktivieren der Netzwerkkarte die Kommunikation mit anderen Geräten im Netzwerk zu stoppen, klicken Sie auf **Deaktivieren**. Wenn die Netzwerkverbindung deaktiviert ist, erscheint eine Meldung auf dem Gerät, die besagt, dass die Netzwerkkarte deaktiviert wurde.
4. Wenn das Gerät wieder bedenkenlos mit dem Netzwerk verbunden werden kann, klicken Sie auf **Aktivieren**. Wenn die Verbindung wiederhergestellt ist, erscheint eine Meldung auf dem Gerät, die besagt, dass die Netzwerkkarte wieder aktiviert ist.

Öffnen des Intel AMT-Konfigurationsbildschirms

System Manager enthält eine Verknüpfung, über die Sie den Intel AMT-Konfigurationsbildschirm öffnen können. Es handelt sich dabei um eine von Intel bereitgestellte Oberfläche, die es ermöglicht, den Gerätestatus, Hardwareinformationen, das Intel AMT-Ereignisprotokoll, Remotestartoptionen und Netzwerkeinstellungen anzuzeigen. Darüber hinaus können Sie in dieser Oberfläche AMT-Benutzerkonten für das Gerät hinzufügen und bearbeiten. Das Fenster, in dem dieser Bildschirm angezeigt wird, ist von der System Manager-Konsole getrennt. Falls Sie

Fragen zur Verwendung dieser Benutzeroberfläche haben, sollten Sie sich an den technischen Support des Geräteherstellers wenden.

So öffnen Sie den Intel AMT-Konfigurationsbildschirm

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie im Konsolenfenster des Geräts auf **Intel AMT-Optionen**.
3. Klicken Sie auf **Intel AMT-Konsole** und klicken Sie dann auf **Intel AMT-Webkonsole starten**.

Rollenbasierte Administration

Informationen zur rollenbasierten Administration

Verwenden Sie die rollenbasierte Administration, um den Zugriff der Benutzer auf Produkt-Tools und andere Geräte auf der Basis ihrer administrativen Funktion in Ihrem System zu konfigurieren. In der rollenbasierten Administration entscheiden Sie mithilfe von Bereichen, welche Geräte bestimmte Benutzer anzeigen und verwalten können; darüber hinaus legen Sie durch die Erteilung von Nutzungsrechten fest, welche Tasks die Benutzer ausführen können.

Administratoren (Benutzer mit Administratorrecht) können auf die Tools der rollenbasierten Administration zugreifen, indem sie auf **Benutzer** im linken Navigationsfenster klicken.

Mithilfe der rollenbasierten Administration können Sie Benutzern des Produkts, abhängig von ihren Rechten und ihrem Bereich, administrative Rollen zuweisen. Die *Rechte* legen fest, welche Produkt-Tools und -Funktionen der Benutzer sehen und verwenden kann. Der *Bereich* bestimmt, welche Geräte der Benutzer sehen und verwalten kann.

Die von Ihnen erstellten Rollen können auf den Verantwortungsbereichen der Benutzer basieren, den Verwaltungstasks, deren Ausführung Sie den Benutzern gestatten möchten, und den Geräten, auf die die Benutzer zugreifen und die sie verwalten sollen. Der Gerätezugriff lässt sich auf einen Standort, beispielsweise ein Land, eine Region, ein Bundesland, eine Stadt oder sogar ein bestimmtes Büro oder eine Abteilung, einschränken. Der Zugriff kann auch auf eine bestimmte Plattform, einen Prozessortyp oder andere Hard- und Softwareattribute der Geräte eingeschränkt werden. Bei der rollenbasierten Administration können Sie frei entscheiden, wie viele Rollen Sie erstellen möchten, welche Benutzer diese Rollen wahrnehmen können und wie groß oder klein der Gerätezugriffsbereich sein soll.

Beispiele für administrative Rollen

Die folgende Tabelle beschreibt Folgendes: Die möglichen administrativen Rollen, die von Ihnen nach Bedarf implementiert werden können, die von den Benutzern ausgeführten gängigen Tasks und die Rechte, die Benutzer benötigen, um die betreffende Rolle effektiv ausfüllen zu können.

Rolle	Aufgaben	Erforderliche Rechte
Administrator	Konfiguration von Core Servern, Benutzerverwaltung, Konfiguration von Warnmeldungen, Integration von Produkten anderer Unternehmen etc. (Administratoren mit vollen Rechten können zudem jeden beliebigen Verwaltungstask ausführen).	Administrator (mit allen Rechten)
Inventarverwaltung	Erkennung von Geräten, Konfiguration von Geräten, Ausführung des Inventarscanners,	Geräteerkennung, Softwareverteilung und

Rolle	Aufgaben	Erforderliche Rechte
	Aktivierung der Nachverfolgung für den Inventarverlauf etc.	Verwaltung öffentlicher Abfragen
Berichtsverwalter	Ausführen von vordefinierten Berichten, Drucken von Berichten etc.	Berichte (erforderlich für alle Berichte)

Dies sind nur Beispielrollen. Die rollenbasierte Administration besitzt die Flexibilität, Sie so viele benutzerdefinierte Rollen erstellen zu lassen, wie Sie möchten. Sie können dieselben Rechte auch verschiedenen Benutzern zuweisen, den Zugriff dieser Benutzer jedoch auf eine begrenzte Gruppe von Geräten (reduzierter Bereich) limitieren. Sogar ein Administrator kann durch einen Bereich eingeschränkt werden, indem seine Administratoraufgaben auf eine bestimmte geographische Region oder einen bestimmten Typ von verwalteten Geräten eingeschränkt wird. Wie Sie am besten von der rollenbasierten Administration profitieren, hängt von Ihren Netzwerk- und Personalressourcen und Ihrem individuellen Unternehmensbedarf ab.

Um die rollenbasierte Administration zu implementieren und durchzusetzen, müssen Sie lediglich aktuelle lokale Windows-Benutzer (oder erstellen Sie neue Windows-Benutzer und fügen Sie sie hinzu) als Produktbenutzer angeben, die Benutzer der Management Suite-Benutzergruppe hinzufügen und dann die erforderlichen Rechte (für Produktfunktionen) und Bereiche (verwaltete Geräte) zuweisen. Folgen Sie den Anweisungen in den nachstehenden Kapiteln:

Grundlegendes zu den Rechten

Über die Rechte erhalten Sie Zugriff auf bestimmte Tools und Funktionen. Benutzer müssen über das erforderliche Recht (oder Rechte) verfügen, um entsprechende Aufgaben durchzuführen. Um Geräte im Bereich eines Benutzers fernzusteuern, muss ein Benutzer über das Fernsteuerungsrecht verfügen. Wenn Sie mehrere LANDesk-Verwaltungsprodukte installiert haben, können Rechte von jeder Konsole aus zugewiesen werden und die Bereiche sind auf allen Konsolen wirksam.

Wenn ein Recht einem Benutzer nicht zugewiesen wird, werden diesem Benutzer mit diesem Recht verknüpfte Tools nicht in der Produktkonsole angezeigt. Beispiel: Wenn einem Benutzer das Recht zur Berichterstellung nicht erteilt wurde, wird das Berichtelement nicht nicht im linken Navigationsfenster angezeigt. Die unten aufgeführte Tabelle zeigt, welche Rechte der Benutzer zum Anzeigen des Tools benötigt.

Tool	Erforderlichen Rechten zum Anzeigen im linken Navigationsfenster
Eigene Geräte	Einfache Webkonsole
Agentenkonfiguration	Administrator
Alarmfunktion	Alarmierung und Überwachung

Tool	Erforderlichen Rechten zum Anzeigen im linken Navigationsfenster
Geräteerkennung	Geräteerkennung
Überwachung	Alarmierung und Überwachung
Abfragen	Einfache Webkonsole, Verwaltung öffentlicher Abfragen, Berichte
Berichte	Berichte, Patch-Management
Geplante Tasks	Geräteerkennung
Skripte	Patch-Management
Benutzer	Administrator
Software-Updates	Patch-Management
Voreinstellungen	Einfache Webkonsole
Hardwarekonfiguration	Administrator

In den nachfolgenden Abschnitten erfahren Sie mehr über die einzelnen Produktrechte und darüber, wie Rechte verwendet werden können, um administrative Rollen zu erstellen.

Bereiche steuern den Zugriff auf Geräte
Wenn die Funktionen verwendet werden, die durch diese Rechte freigegeben sind, werden Benutzer stets durch ihren Bereich eingeschränkt (die Geräte, die sie sehen und beeinflussen können).

Administrator

Das Administratorrecht gewährt uneingeschränkten Zugriff auf alle Produkttools (die Verwendung dieses Tools ist jedoch immer noch auf die Geräte beschränkt, die zum Bereich des Administrators gehören).

Dies ist das Standardrecht für einen neu hinzugefügten Benutzer, sofern Sie die Einstellungen für den "Standardvorlagenbenutzer" nicht geändert haben.

Mit dem Administratorrecht erhalten Benutzer folgende Möglichkeiten:

- Anzeige und Zugriff auf **Benutzer** im linken Navigationsfenster
- Siehe Produktlizenzierung unter **Einstellungen** im linken Navigationsfenster
- Durchführen aller Produkttasks, die durch die anderen unten aufgeführten Rechte zulässig sind

Es wird nicht empfohlen, den Administrator zu löschen. Wenn Sie sich als letzter Administrator bei einer bestimmten LDSM-Konsole angemeldet haben, zum Windows Computer Management wechseln und den Benutzer "Administrator" aus der Management Suite-Gruppe löschen, können beim erneuten Öffnen der Konsole Probleme auftreten. Sie sind zwar für weitere 20 Minuten (das Standard-Sitzungstimeout) als Administrator angemeldet, jedoch stehen Ihnen beim Initiieren von Aktionen oder beim Aktualisieren des Konsolenbrowsers (F5-Taste), bei dem Sie als Administrator angemeldet sind, die exklusiv für den Administrator geltenden Rechte nicht mehr zur Verfügung. Aus diesem Grund sollte der letzte Administrator unter keinen Umständen gelöscht werden.

Hinweise zu den Rechten und Tools
Das Administratorrecht ist exklusiv mit dem Tool **Benutzer** verknüpft. Wenn ein Benutzer das Administratorrecht nicht besitzt, wird dieses Tool nicht in der Konsole angezeigt.

Alle Tools in der Produktkonsole sind mit einem entsprechenden Recht verknüpft (siehe Beschreibung weiter unten).

Geräteerkennung

Das Recht "Geräteerkennung" unterstützt Benutzer bei folgenden Aktionen:

- Suchen nach Geräten im Netzwerk, die keinen Inventarscan an die Core-Datenbank des Produkts weitergeleitet haben, beispielsweise im Rahmen eines Netzwerkscans, einer Standard Management Agent- und einer IPMI-Erkennung.
- Planen von regelmäßig wiederholten Erkennungen
- Verschieben der Geräte von "Erkannt" nach "Verwaltet"

Verwaltung öffentlicher Abfragen

Das Recht "Verwaltung öffentlicher Abfragen" unterstützt Benutzer bei folgenden Aktionen:

- Abfragen erstellen, die allen Benutzern zur Verfügung stehen
- Öffentliche Abfragen erstellen oder löschen
- Vorhandene öffentliche Abfragen ändern/bearbeiten

Berichte

Das Berichtsrecht unterstützt Benutzer bei folgenden Aktionen:

- Anzeige und Zugriff auf das Tool **Berichte** im linken Navigationsfenster
- Ausführen von vordefinierten Berichten

Patch-Management

Das Patch-Management-Recht gilt speziell für die Funktion des Anfälligkeitsscanners. Weitere Informationen finden Sie unter Verwenden von Softwareaktualisierungstools.

Einfache Webkonsole

Das Recht "Einfache Webkonsole" gibt Benutzern die Möglichkeit, die mit diesem Recht verknüpften Funktionen auszuführen. Die Funktionen werden unten aufgeführt (einschließlich etwaiger Ausnahmen innerhalb der Funktion).

- **Eigene Geräte** (das Recht unterstützt nicht das Aktualisieren öffentlicher Gruppen oder Löschen von Geräten auf der Registerkarte **Aktionen**)
- Einstellungen ändern (jedoch keine benutzerdefinierten Attribute)

Alarmierung und Überwachung

Das Alarmierungs- und Überwachungsrecht unterstützt Benutzer bei folgenden Aktionen:

- Überwachen der Leistung unterschiedlicher Systeme und Betriebssystemkomponenten, beispielsweise Laufwerke, Prozessoren, Speicher, Prozesse, vom Webserver des Systems übertragene Byte/Sek. usw.
- Überwachen des Zustands aller verwalteten Geräte
- Anpassen von Alarmmeldungen, die abhängig vom Schweregrad (Kritisch, Warnung, Zu Informationszwecken, OK, Unbekannt) oder einem Grenzwert (z. B., wenn die Festplattenkapazität zu über 90% erschöpft ist) zu senden sind.
- Wählen Sie die Alarmaktion aus, die nach Überschreitung eines Grenzwertes initiiert werden soll (Eintrag im Protokoll, E-Mail-Nachricht, Ausführen eines Programms auf dem Core oder einem bestimmten Gerät, Senden einer SNMP-Trap an eine SNMP-Verwaltungskonsole im Netzwerk).

Hinzufügen von Produktbenutzern

Produktbenutzer sind Benutzer, die sich an der Produktkonsole anmelden und bestimmte Aufgaben für bestimmte Geräte im Netzwerk ausführen können.

Produktbenutzer werden nicht in der Konsole erstellt. Die Benutzer werden stattdessen auf der Registerkarte **Benutzer** angezeigt (im linken Navigationsfenster auf **Benutzer** klicken), nachdem sie der LANDesk Management Suite-Gruppe in der Windows-Benutzerumgebung auf dem Core Server hinzugefügt wurden. Die Gruppe **Benutzer** zeigt alle Benutzer an, die gegenwärtig in der LANDesk Management Suite-Gruppe auf dem Core Server vorhanden sind.

Die Gruppe **Benutzer** beinhaltet zwei Standardbenutzer:

- **Standardvorlagenbenutzer:** Dieser Benutzer ist im Grunde eine Vorlage für Benutzereigenschaften (Rechte und Bereich), die für die Konfiguration neuer Benutzer verwendet wird, wenn diese der LANDesk Management Suite-Gruppe hinzugefügt werden. Wenn Sie dieser Gruppe in der Windows-Umgebung einen Benutzer hinzufügen, erbt dieser Benutzer demnach die Rechte und Bereiche, die aktuell in den Eigenschaften "Standardvorlagenbenutzer" definiert sind. Wenn für den Standardvorlagenbenutzer alle Rechte und der "Standardbereich: Alle Geräte" ausgewählt wurden, werden alle der LANDesk Management Suite-Gruppe neu hinzugefügten Benutzer der Gruppe **Benutzer** hinzugefügt, wobei diese dann automatisch über die Rechte für alle Produkt-Tools und für den Zugriff auf alle Geräte verfügen.

  Sie können die Eigenschaftseinstellungen für den Standardvorlagenbenutzer ändern, indem Sie mit der rechten Maustaste auf diesen Benutzer klicken und dann auf **Rechte bearbeiten** klicken. Wenn Sie z. B. eine große Anzahl von Benutzern gleichzeitig hinzufügen möchten, von denen jedoch nicht alle Zugriff auf alle Tools oder Geräte erhalten sollen, ändern Sie zuerst die Einstellungen für den "Standardvorlagenbenutzer" und fügen dann die Benutzer der LANDesk Management Suite-Gruppe hinzu (siehe unten beschriebene Schritte).

  Der Standardvorlagenbenutzer kann nicht entfernt werden).

- **Standard-Administrator:** Dies ist der Administrator, der am Server angemeldet war, als der Core dieses Produkts installiert wurde.

Wenn Sie einen Benutzer der LANDesk Management Suite-Gruppe in Windows hinzufügen, wird der Benutzer automatisch in die Gruppe **Benutzer** im Fenster **Benutzer** eingelesen und erbt dieselben Rechte und denselben Bereich wie der aktuelle "Standardvorlagenbenutzer". Es werden der Name, der Bereich und die Rechte des Benutzers angezeigt.

Wenn Sie einen Benutzer aus der LANDesk Management Suite-Gruppe in der Windows-Benutzerumgebung entfernen, ist der Benutzer kein aktiver Benutzer mehr und kann aus der Gruppe **Benutzer** entfernt werden. Das Konto des Benutzers existiert weiterhin auf dem Server und kann jederzeit wieder der LANDesk Management Suite-Gruppe hinzugefügt werden. Außerdem bleiben die Untergruppen des Benutzers unter **Benutzergeräte**, **Benutzerabfragen**, **Benutzerberichte** und **Benutzerskripte** erhalten, damit Sie den Benutzer wiederherstellen können, ohne die in diesen Gruppen gespeicherten Daten zu verlieren, und damit Sie Daten nach Bedarf auf andere Benutzer kopieren können.

Um die Liste **Benutzer** zu aktualisieren und damit etwaige neu hinzugefügte Benutzer anzuzeigen, klicken Sie auf **Benutzer** und dann auf die Schaltfläche **Aktualisieren** Ihres Browsers.

So fügen Sie einen Benutzer oder eine Domänengruppe der LANDesk Management Suite-Gruppe hinzu

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Gruppen** des Servers.
2. Klicken Sie mit der rechten Maustaste auf die **LANDesk Management Suite**-Gruppe und klicken Sie dann auf **Zur Gruppe hinzufügen**.
3. Klicken Sie auf **Hinzufügen**, geben Sie dann einen Benutzer ein oder wählen Sie mindestens einen Benutzer in der Liste aus.

4. Klicken Sie auf **Hinzufügen** und **OK**.

Hinweis: Sie können einen Benutzer der LANDesk Management Suite-Gruppe hinzufügen, indem Sie mit der rechten Maustaste auf das Benutzerkonto in der Benutzerliste klicken; klicken Sie auf **Eigenschaften | Mitglied von** und auf **Hinzufügen**, um die Gruppe auszuwählen und den Benutzer hinzuzufügen.

Wenn in Windows noch keine Benutzerkonten vorhanden sind, müssen Sie sie zuerst auf dem Server erstellen.

So erstellen Sie ein neues Benutzerkonto

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Benutzer** des Servers.
2. Klicken Sie mit der rechten Maustaste auf **Benutzer** und auf **Neuer Benutzer**.
3. Geben Sie im Dialogfeld "Neuer Benutzer" einen Namen und ein Kennwort ein.
4. Legen Sie die Kennworteinstellungen fest.
5. Klicken Sie auf **Erstellen**. Das Dialogfeld "Neuer Benutzer" bleibt geöffnet, sodass Sie zusätzliche Benutzer erstellen können.
6. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.
7. Fügen Sie den Benutzer der LANDesk Management Suite-Gruppe hinzu, damit er in der Gruppe "Benutzer" in der Konsole angezeigt wird.

Sie können nun die Produkt!-Benutzerrechte und den Bereich zuweisen.

Erstellen von Bereichen

Ein Bereich definiert die Geräte, die von einem Benutzer des Produkts angezeigt und verwaltet werden können. Wenn Sie mehrere LANDesk-Verwaltungsprodukte installiert haben, können Bereiche von jeder Konsole aus zugewiesen werden und die Bereiche sind auf allen Konsolen wirksam.

Ein Bereich kann beliebig groß oder klein sein, alle in eine Core-Datenbank gescannten und verwalteten Geräte umfassen, sich nur auf ein einziges Gerät erstrecken oder keine Geräte enthalten. Diese Flexibilität, kombiniert mit dem modularen Tool-Zugriff, macht aus der rollenbasierten Administration eine vielseitige Verwaltungsfunktion.

Standardbereiche

Die rollenbasierte Administration umfasst zwei Standardbereiche. Diese beiden folgenden Bereiche können beim Konfigurieren der Benutzereigenschaften des Standardvorlagenbenutzers nützlich sein.

- **(Standard) Bereich "Kein Rechner":** Schließt alle Geräte in der Datenbank aus.
- **(Standard) Bereich "Alle Rechner":** Schließt alle Geräte in der Datenbank ein.

Sie können die Standardbereiche weder bearbeiten noch entfernen.

Benutzerdefinierte Bereiche

Sie können folgende benutzerdefinierten Bereiche erstellen und Benutzern zuweisen:

- **Abfragebasiert:** Beschränkt den Zugriff auf diejenigen Geräte, die einer benutzerdefinierten Abfragesuche entsprechen. Um einen Bereich zu definieren, können Sie eine vorhandene Abfrage auswählen oder im Dialogfeld **Abfrage** eine neue Abfragen erstellen. Weitere Informationen zum Erstellen von Abfragen finden Sie unter Erstellen von Datenbankabfragen.
- **Gruppenbasiert:**Regelt nur den Zugriff auf Geräte, die sich in der ausgewählten Gruppe befinden. Sie können Gruppen aus dem Dialogfeld **Eigenschaften des Gruppenbereichs** auswählen, um einen Bereich zu definieren.

Sie können jedem Benutzer nach Bedarf mehrere Bereiche zuweisen. Wenn einem Benutzer mehrere Bereiche zugewiesen werden, ist der geltende kumulative Bereich (d. h., das vollständige Spektrum an Geräten, das als Folge des Zusammenfassens mehrerer zugewiesener Bereiche geöffnet und verwaltet werden kann) ein Verbund.

Sie können den zusammengefassten Bereich eines Benutzers jederzeit ändern, indem Sie Bereiche hinzufügen und entfernen. Alle Bereichstypen lassen sich miteinander kombinieren.

So erstellen Sie einen Bereich

1. Klicken Sie im linken Navigationsfenster auf **Benutzer**.
2. Klicken Sie auf der Registerkarte **Bereich** auf die Symbolleistenschaltflächen **Neuer Abfragebereich** oder **Neuer Gruppenbereich**.
3. Geben Sie einen Namen für den neuen Bereich ein.
4. Wenn Sie abfragebasiert ausgewählt hatten, wählen Sie eine vorhandene Abfrage aus, oder klicken Sie auf **Definieren**, um eine neue Abfrage zu erstellen. Klicken Sie auf **OK**.
5. Wenn Sie gruppenbasiert ausgewählt hatten, wählen Sie eine Gruppe aus und klicken auf **OK**.
6. Klicken Sie auf **OK**, um den Bereich zu speichern und das Dialogfeld zu schließen.

Zuweisen von Rechten und Bereiche an Benutzer

- Informationen zum Dialogfeld "Benutzerrechte/Bereich"
- Informationen zum Dialogfeld "Fernsteuerungseinstellungen"

In den bisherigen Abschnitten wurde beschrieben, wie Sie Produktbenutzer hinzufügen, welche Bedeutung Rechte haben, wie Rechte den Zugriff auf Funktionen und Tools steuern und wie Sie Gerätebereiche erstellen, um den Zugriff auf verwaltete Geräte zu gewähren oder einzuschränken. Der nächste Schritt bei der Einrichtung der rollenbasierten Administration besteht darin, jedem Benutzer die entsprechenden Rechte und einen Bereich zuzuweisen.

Sie können die Rechte und den Bereich eines Benutzers jederzeit ändern.

Die geänderten Rechte oder Bereiche eines Benutzers werden erst wirksam, wenn der betreffende Benutzer sich das nächste Mal bei der Konsole anmeldet.

So weisen Sie Rechte und einen Bereich zu

1. Klicken Sie im linken Navigationsfenster auf **Benutzer**.
2. Erweitern Sie die Liste der Benutzer, um alle Benutzer anzuzeigen, die zurzeit der Gruppe "LANDesk Management Suite" in der Windows NT-Umgebung des Core Servers angehören.

   Diese Liste enthält Benutzernamen und zugewiesene Rechte (ein Häkchen gibt an, dass das Recht aktiviert ist).

3. Klicken Sie mit der rechten Maustaste auf einen Benutzer und dann auf **Bearbeiten**.
4. Aktivieren oder deaktivieren Sie Rechte nach Bedarf im Dialogfeld **Benutzer/Bereich**.
5. Klicken Sie auf die Registerkarte **Bereich** und wählen Sie einen Bereich aus der Liste **Zugewiesene Bereiche** aus.
6. Klicken Sie auf **Übernehmen**.

Die neuen Rechte werden neben dem Namen des Benutzers in der Liste angezeigt. Sie werden wirksam, wenn der Benutzer das nächste Mal eine Verbindung mit dem Core Server herstellt.

So löschen Sie einen Bereich

1. Klicken Sie im linken Navigationsfenster auf **Benutzer**.
2. Klicken Sie auf die Registerkarte **Bereich** und klicken Sie auf den Bereich, den Sie löschen möchten, und klicken Sie dann auf **Löschen**. Klicken Sie auf **OK**.

Gehen Sie beim Löschen von Bereichen umsichtig vor. Die Benutzer, die den von Ihnen gelöschten Bereichen zugewiesen waren, erhalten durch das Wegfallen des Bereichs Zugriff auf Rechte, die ihnen bisher durch den Bereich verwehrt wurden.

Informationen zum Dialogfeld "Benutzerrechte/Bereiche"

Verwenden Sie dieses Dialogfeld, um die zugewiesenen Rechte und den zugewiesenen Bereich eines Benutzers anzuzeigen. Öffnen Sie das Dialogfeld, indem Sie einen Benutzer auswählen und auf **Rechte bearbeiten** klicken.

Registerkarte "Rechte": Listet die dem Benutzer erteilten Rechte auf.

- **Administrator**
- **Geräteerkennung**
- **Verwaltung öffentlicher Abfragen**
- **Berichte**
- **Patch-Management**
- **Einfache Webkonsole**
- **Alarmierung und Überwachung**

Registerkarte "Bereich": Listet die dem Benutzer zugewiesenen Bereiche auf.

- **Zugewiesene Bereiche:** Benennt die aktuellen Bereiche des Benutzers.
- **Hinzufügen:** Öffnet das Dialogfeld **Bereich hinzufügen**; in diesem Dialogfeld können Sie einen Bereich auswählen und dem Benutzer zuweisen.
- **Entfernen:** Löscht den ausgewählten Bereich.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Geräteerkennung

Verwenden der Geräteerkennung

Die Geräteerkennung findet Geräte in Ihrem Netzwerk, auf denen keine Agenten des Erkennungs-Cores installiert sind und die keinen Inventarscan an dieselbe Core-Datenbank gesendet haben. Die Geräteerkennung verwendet mehrere Methoden, um Geräte in Ihrem Netzwerk ausfindig zu machen.

- **Netzwerkscan:** Sucht mithilfe einer ICMP-Ping-Suche nach Computern. Dies ist die gründlichste, jedoch auch zeitaufwendigste Suche (verwendet IP-Fingerprinting-Technologie). Sie können die Suche auf bestimmte IP- und Subnetzbereiche beschränken. Diese Option setzt standardmäßig NetBIOS ein, um Informationen über das Gerät zu sammeln. Sie können auch "IP-Fingerabdruck" auswählen; hiermit wird (in den meisten Fällen) der Betriebssystemtyp erkannt. Die Netzwerkscanoption verfügt außerdem über die Option **SNMP verwenden**. Mit dieser Option können Sie festlegen, dass der Scan SNMP für SNMP-Geräte (beispielsweise einzelne Drucker) benutzt.
- **CBA-Erkennung:** Sucht auf Computern nach dem Standard Management Agent (der frühere Common Base Agent [CBA] in Management Suite). Diese Option erkennt Computer, die von Server Manager, System Manager usw. verwaltet wurden. Sie können die PDS2-Option auswählen, um Geräte mithilfe des älteren LANDesk PDS2-Agenten zu erkennen. CBA-Erkennung wird für Linux-Rechner nicht unterstützt. Wenn Sie jedoch PDS2 auswählen, können Linux-Rechner, auf denen ein Agent installiert ist, erkannt werden.
- **IPMI:** Sucht nach Servern mit aktiviertem Intelligent Platform Management Interface. Damit können Sie auf den Baseboard Management Controller (BMC) zugreifen, unabhängig davon, ob der Server eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet.
- **Servergehäuse:** Sucht nach Blade-Server Chassis Management Modules (CMMs). Die Blades in den Servern werden als normale Server erkannt.
- **Intel* AMT:** Sucht nach Geräten mit Intel Active Management Technology (Version 1). Damit können Sie auf eine begrenzte Anzahl von Verwaltungsfunktionen zugreifen, unabhängig davon, ob der Server eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet.

Die Geräteerkennung versucht, für jedes Gerät die wichtigsten Daten ausfindig zu machen. Nicht alle der unten angezeigten Informationen sind für jedes Gerät verfügbar.

- **Knotenname:** Der Name des erkannten Geräts, falls verfügbar.
- **IP-Adresse:** Die ermittelte IP-Adresse.
- **Subnetzmaske:** Die ermittelte Subnetzmaske.
- **Kategorie:** Die Geräteerkennungsgruppe, der das Gerät angehört.
- **Betriebssystemname:** Die erkannte Betriebssystembeschreibung, falls verfügbar.

Wenn die Geräteerkennung ein Gerät erstmalig findet, prüft sie in der Core-Datenbank nach, ob die IP-Adresse und der Name des Geräts bereits in der Datenbank in der Liste **Eigene Geräte** vorhanden sind. Ein Gerät in der Liste **Nicht verwaltet** wird wieder erkannt und liefert potenziell weitere Daten. Wenn es eine Übereinstimmung gibt, ignoriert die Geräteerkennung das Gerät.

Gibt es keine Übereinstimmung, fügt die Geräteerkennung das Gerät in die Tabelle **Nicht verwaltete Geräte** ein. Geräte in der Tabelle **Nicht verwaltet** verwenden keine System Manager-Lizenz. Ein Gerät gilt als verwaltet, sobald es einen Inventarscan an die Core-Datenbank sendet. Sobald Sie ein Gerät in die Gruppe **Alle Geräte** verschoben haben, wird es nicht mehr in der Liste **Erkannte Geräte** angezeigt.

IPMI-Geräte müssen über einen konfigurierten BMC (Baseboard Management Controller) verfügen, damit sie als IPMI-Geräte erkannt werden und die IPMI-Funktionalität in vollem Umfang nutzen können. Wenn der BMC nicht konfiguriert ist, können Sie das Gerät als Computer erkennen lassen. Anschließend können Sie das Gerät zur Liste mit den verwalteten Geräten hinzufügen und mithilfe der Funktion "Hardware-Konfiguration" das BMC-Kennwort konfigurieren. Die IPMI-Funktionalität des Geräts wird dann von diesem Produkt erkannt. Beachten Sie, dass die IP-Adresse des BMC nicht notwendigerweise mit der IP-Adresse des Betriebssystems übereinstimmt und deshalb u. U. kein direkter Agenten-Push-Vorgang auf die IP-Adresse des BMC ausgeführt werden kann. Eine Neuerkennung von Standard-IPs ist ggf. erforderlich, um einen Push-Vorgang auf die IP des BMCs mithilfe eines Standardagenten durchzuführen. Die BMC IP sollte in der Lage sein, einen IP-Agenten-Push entgegenzunehmen.

Mit Intel* AMT (Version 1) aktivierte Geräte sollten mit einem Intel AMT-Benutzernamen und Kennwort konfiguriert werden, um als Intel AMT-Geräte identifiziert und erkannt zu werden. Nach Abschluss der Erkennung können Sie die Funktion "Hardware-Konfiguration" ausführen, um die Intel AMT-Einstellungen zu konfigurieren und das Gerät im Small Business- oder im sicheren Enterprise-Modus bereitzustellen.

Um die Geräteerkennung zu automatisieren, können Sie regelmäßige Erkennungsvorgänge planen. Sie können beispielsweise Ihr Netzwerk in Subnetze unterteilen und zeitplangesteuert für jedes einzelne Subnetz eine Ping-Suche pro Nacht durchführen. In allen Erkennungen übernimmt der Core Server die Suche.

Für die Erkennung und Verwaltung von Geräten in Ihrem Netzwerk, müssen Sie folgende Tasks ausführen:

- Erkennungskonfigurationen erstellen
- Den Erkennungsvorgang planen und ausführen
- Erkannte Geräte anzeigen
- Erkannte Geräte in die Liste **Eigene Geräte** verschieben

Verwenden der Funktion "Erkennung nicht verwalteter Geräte" mit Firewall-geschützten Geräten

Denken Sie daran, dass die "Erkennung nicht verwalteter Geräte" im Normalfall keine Geräte erkennt, die eine Firewall verwenden (z. B. die Windows-Firewall), es sei denn, Sie konfigurieren die Firewall manuell. Sie müssen die folgenden Anschlüsse öffnen: Greifen Sie über die Systemsteuerung auf die Windows-Firewall zu, um diese Einstellungen zu ändern.

Verwaltete Server:

- Datei- und Druckerfreigabe: TCP 139, 445; UDP 137,138 (unabdingbare Voraussetzung für den Push-Prozess)
- Softwareverteilung: TCP 9595 (unabdingbare Voraussetzung für den Push-Prozess)

- Erweitert - ICMP: "Allow incoming echo request" (Kann nicht erkannt werden, wenn diese Einstellung nicht aktiviert ist.)

Core Server:

- Inventar: 5007
- Fernsteuerung: 9535

Erstellen von Erkennungskonfigurationen

Verwenden Sie die Registerkarte **Erkennungskonfigurationen**, um neue Erkennungskonfigurationen zu erstellen, vorhandene Konfigurationen zu bearbeiten und zu löschen und eine Konfiguration für einen Erkennungsvorgang zu planen. Jede Erkennungskonfiguration besteht aus einem beschreibenden Namen, den zu scannenden IP-Bereichen und dem Erkennungstyp.

Nachdem Sie eine Konfiguration erstellt haben, können Sie mit dem Dialogfeld **Erkennung planen** festlegen, wann sie ausgeführt werden soll.

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Klicken Sie auf der Registerkarte **Erkennungskonfigurationen** auf die Schaltfläche **Neu**.
3. Füllen Sie die unten beschriebenen Felder aus. Klicken Sie, nachdem Sie alle Daten eingegeben haben, auf die Schaltfläche **Hinzufügen** und dann auf **OK**.

Im Folgenden werden die einzelnen Abschnitte des Dialogfelds **Erkennungskonfiguration** beschrieben.

- **Konfigurationsname:** Geben Sie einen Namen für die Konfiguration ein. Geben Sie der Konfiguration einen Namen, den Sie sich leicht merken können. Die Konfiguration kann bis zu 255 Zeichen umfassen; folgende Zeichen sind unzulässig: **"**, **+**, **#**, **&** oder **%.** Der Konfigurationsname wird nach Verwendung eines dieser Zeichen nicht mehr angezeigt.
- **Standard-Netzwerkscan:** Diese Option sucht nach Geräten, indem sie ICMP-Pakete an die IP-Adressen in dem von Ihnen angegebenen Bereich sendet. Diese Suche ist am gründlichsten, verursacht jedoch auch den größten Zeitaufwand. Diese Option verwendet standardmäßig NetBIOS, um Informationen zum Gerät zu sammeln.

  Die Scanoption des Netzwerks verfügt über einen **IP-Fingerabdruck**, mit dem die Geräteerkennung versucht, den Betriebssystemtyp über TCP-Paketantworten ausfindig zu machen. Der IP-Fingerabdruck verlangsamt die Erkennung geringfügig.

  Die Scanoption des Netzwerks verfügt darüber hinaus über die Option **SNMP verwenden** , mit der Sie den Scan für die Verwendung von SNMP konfigurieren können. Klicken Sie auf **Konfigurieren**, um Informationen zu Ihrer SNMP-Konfiguration einzugeben. Weitere Informationen finden Sie unter Konfigurieren von SNMP-Scans.

- **LANDesk CBA-Erkennung:** Sucht nach dem Standard Management Agent (der frühere Common Base Agent [CBA] in Management Suite) auf Geräten. Mit dem Standard Management Agent kann der Core Server nach Clients im Netzwerk suchen und mit ihnen kommunizieren. Diese Option erkennt Geräte, auf denen Produktagenten installiert sind. Router blockieren durch den Standard Management Agent und PDS2 bedingten Datenverkehr. Um eine Standard-CBA-Erkennung über mehrere Subnetze hinweg durchzuführen, muss der Router so konfiguriert sein, dass an mehrere Subnetze gerichtete Broadcasts unterstützt werden.

  Die CBA-Erkennungsoption verfügt zudem über eine **LANDesk PDS2-Erkennungsoption**, mit der die Geräteerkennung nach dem LANDesk Ping Discovery Service (PDS2) auf Geräten sucht. LANDesk Softwareprodukte wie LANDesk® System Manager, Server Manager und LANDesk Client Manager verwenden den PDS2-Agenten. Wählen Sie diese Option aus, wenn es in Ihrem Netzwerk Geräte gibt, auf denen diese Produkte installiert sind. CBA-Erkennung wird für Linux-Rechner nicht unterstützt. Wenn Sie jedoch PDS2 auswählen, können Linux-Rechner, auf denen ein Agent installiert ist, erkannt werden.
- **IPMI:** Sucht nach IPMI-fähigen Servern. IPMI ist eine von Intel, ***** H-P,* NEC,* und Dell* entwickelte Norm, die die Nachrichten- und Systemschnittstelle für verwaltbare Hardwarebestandteile definiert. IPMI bietet Überwachungs- und Wiederherstellungsfunktionen, mit denen Sie auf diese Funktionen zugreifen können, ganz gleich, ob das Gerät eingeschaltet ist oder nicht, und in welchem Zustand das Betriebssystem sich befindet. Denken Sie daran, dass das Gerät nicht auf ASF-Pings reagiert, wenn der Baseboard Management Controller nicht konfiguriert ist. Das Produkt verwendet ASF-Pings zum Erkennen von IPMI. Das heißt, dass Sie das Produkt als normalen Computer erkennen lassen müssen. Beim Push-Bereitstellen des Clients durchsucht ServerConfig das System, erkennt das Gerät als IPMI und konfiguriert den BMC. Eine Übersicht über IPMI finden Sie unter IPMI-Support.
- **Servergehäuse:** Sucht nach Blade-Server Chassis Management Modules (CMMs). Die Blades in den Servern werden als normale Server erkannt.
- **Intel* AMT:** Sucht nach Geräten mit Intel Active Management Technology-Unterstützung.
- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Letzte IP-Adresse:** Geben Sie die Abschluss-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Subnetzmaske:** Geben Sie die Subnetzmaske für den IP-Adressbereich ein, den Sie überprüfen möchten.
- **Hinzufügen:** Fügt den IP-Adressbereich in die Warteschlange im unteren Abschnitt des Dialogfelds ein.
- **Löschen:** Löscht den Inhalt der IP-Adressbereich-Felder.
- **Bearbeiten:** Wählen Sie einen IP-Adressbereich in der Arbeitswarteschlange aus und klicken Sie auf **Bearbeiten**. Der Bereich wird in den Textfelder oberhalb der Arbeitswarteschlange angezeigt. Sie können den Bereich dort bearbeiten und den neuen Bereich zur Arbeitswarteschlange hinzufügen.
- **Entfernen:** Entfernt den ausgewählten IP-Adressbereich aus der Arbeitswarteschlange.
- **Alle entfernen:** Entfernt alle IP-Adressbereiche aus der Warteschlange.

So bearbeiten oder löschen Sie eine Konfiguration

- Klicken Sie auf der Registerkarte **Erkennungskonfigurationen** auf die Konfiguration und dann auf **Bearbeiten** oder **Löschen**.

Konfigurieren von SNMP-Scans

Netzwerkscan-Erkennungen können SNMP verwenden. Abhängig von der SNMP-Konfiguration Ihres Netzwerks müssen Sie u. U. zusätzliche SNMP-Informationen in die Erkennungskonfiguration eingeben. Durch Klicken auf **Konfigurieren** neben der **SNMP**-Option wird das Dialogfeld **SNMP-Konfiguration** angezeigt, das folgende Optionen enthält:

- **Versuche:** Wie oft die Geräteerkennung versucht, die SNMP-Verbindung herzustellen.
- **Auf Antwort warten (Sekunden):** Wie lange die Geräteerkennung auf eine SNMP-Antwort warten soll.
- **Anschluss:** Der Anschluss, an den die Geräteerkennung SNMP-Abfragen senden soll.
- **Community-Name:** Der von der Geräteerkennung zu verwendende SNMP-Community-Name.
- **SNMP V3 konfigurieren:** Die Geräteerkennung unterstützt auch SNMP V3. Klicken Sie auf diese Schaltfläche, um SNMP V3-Optionen im Dialogfeld **SNMP V3-Konfiguration** zu konfigurieren.

Das Dialogfeld **SNMP V3-Konfiguration** enthält folgende Optionen:

- **Benutzername:** Der Benutzername, den die Geräteerkennung für die Authentifizierung gegenüber dem SNMP-Remote-Dienst verwenden sollte.
- **Kennwort:** Das Kennwort für den SNMP-Remote-Dienst.
- **Authentifizierungstyp:** Der von SNMP verwendete Authentifizierungstyp. Kann **MD5**, **SHA** oder **Keiner** sein.
- Privacy-**Typ:** Die vom SNMP-Dienst verwendete Verschlüsselungsmethode. Kann **DES**, **AES128** oder **Keiner** sein.
- Privacy-**Kennwort:** Das mit dem angegebenen Privacy-Typ zu verwendende Kennwort. Nicht verfügbar, wenn Sie für "Privacy-Typ" die Option **Keiner** ausgewählt haben.

Planen und Ausführen des Erkennungsvorgangs

Verwenden Sie die Schaltfläche **Planen** auf der Registerkarte **Erkennungskonfiguration**, um das Dialogfeld **Geplanter Task** anzuzeigen. Legen Sie mithilfe dieses Dialogfelds fest, wann die Erkennung durchgeführt werden soll. Sie können festlegen, dass eine Erkennungskonfiguration sofort, zu einem späteren Zeitpunkt oder zeitplangesteuert (regelmäßig wiederkehrender Vorgang) ausgeführt wird.

Erkennungstasks können auf einen neuen Termin verlegt oder auf der Registerkarte **Erkennungstasks** gelöscht werden. Nachdem Sie eine Erkennung geplant haben, können Sie sich auf der Registerkarte **Erkennungstasks** über den Status der Erkennung informieren. Sie können auch mit dem Tool **Geplante Tasks** auf den Erkennungstask-Status zugreifen. Sobald

eine Erkennung abgeschlossen ist, werden neue Geräte, die sich noch nicht in der Core-Datenbank befinden, der Kategorie "Erkannte Geräte" hinzugefügt.

Das Dialogfeld **Geplanter Task** umfasst folgende Optionen:

- **In globalen Tasks anzeigen:** Lässt zu, dass andere Benutzer den Task sehen. Wenn ein anderer Benutzer den Task bearbeitet oder ausführt, wird dem Benutzer Eigentümerstatus für eine Instanz des Tasks erteilt.
- **Eigentümer:** Der Eigentümer des Tasks.
- **Ungeplant lassen:** (Standard) Bewahrt den Task für künftige Zeitpläne in der Taskliste auf.
- **Jetzt starten:** Führt den Task sobald wie möglich aus. Es kann bis zu einer Minute dauern, bevor der Task gestartet wird.
- **Zum geplanten Zeitpunkt starten:** Startet den Task zu der von Ihnen angegebenen Uhrzeit. Wenn Sie auf diese Option klicken, müssen Sie Folgendes eingeben:
    - **Datum:** Das Datum, an dem der Task gestartet werden soll. Je nach lokalem Standard ist die Datumsreihenfolge entweder Tag-Monat-Jahr oder Monat-Tag-Jahr.
    - **Uhrzeit:** Die Uhrzeit für den Taskbeginn..
    - **Wiederholen alle:** Wenn Sie den Task wiederholt ausführen möchten, wählen Sie ein Intervall aus (täglich, wöchentlich oder monatlich). Wenn Sie "Monat" wählen und das Datum nicht in allen Monaten existiert (beispielsweise der 31.), wird der Task nur in den Monaten ausgeführt, in denen das Datum existiert.

So planen Sie eine Erkennung

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Wählen Sie auf der Registerkarte **Erkennungskonfigurationen** die gewünschte Konfiguration aus und klicken Sie auf **Planen**. Konfigurieren Sie den Erkennungszeitplan. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.
3. Überwachen Sie den Fortschritt des Erkennungsvorgangs auf der Registerkarte **Erkennungstasks**.
4. Zeigen Sie nach Abschluss des Erkennungsvorgangs alle Ergebnisse oben rechts im Fensterausschnitt **Erkannte Geräte** an. Wenn Sie auf den Erkennungstask doppelklicken, wird die Anzahl und der Prozentanteil der Geräte mit 0 angegeben, da diese Zahlen an Zielgeräte geknüpft sind und für Erkennungstasks keine Ziele definiert werden.

Im Fenster **Erkennungstasks** wird der Status des Erkennungstask angezeigt. Der Status beinhaltet folgende Angaben:

- Den Namen der Erkennungskonfiguration.
- Den Taskstatus ("In Arbeit", "Alle Vorgänge abgeschlossen", "Kein Vorgang abgeschlossen" oder "Fehlgeschlagen").
- Wann der Task zum letzten Mal ausgeführt wurde.
- Welcher Tasktyp ausgeführt wurde.

So löschen Sie eine Erkennung oder planen Sie eine erneute Erkennung

Wenn Sie einen Task aus der Liste löschen möchten (ganz gleich, ob er bereits ausgeführt wurde oder nicht), klicken Sie auf den Task und dann auf **Löschen**. Wenn der Task noch nicht

ausgeführt wurde oder wiederholt ausgeführt wird, verhindern Sie durch das Löschen, dass der Task künftig ausgeführt wird.

Sie können die Ausführung eines Erkennungstasks auch auf einen anderen Termin oder eine andere Uhrzeit verschieben, indem Sie auf den Task und dann auf **Bearbeiten** klicken, **Planen** auswählen und den Zeitplan zurücksetzen. Klicken Sie auf **Jetzt starten**, um den Task sofort erneut auszuführen.

So zeigen Sie den Status des Erkennungstask an

1. Klicken Sie im linken Navigationsfenster auf **Erkannte Geräte**.
2. Klicken Sie auf die Registerkarte **Erkennungstasks** oder klicken Sie auf **Aktualisieren** in der Symbolleiste dieses Bereichs.

Anzeigen erkannter Geräte

Zeigen Sie alle erkannten Geräte im oberen Fensterbereich der Funktion **Erkannte Geräte** an. In diesem Fensterbereich werden die Ergebnisse aller Erkennungsvorgänge angezeigt, die Sie ausgeführt haben. Bei jedem neuen Erkennungsvorgang werden gefundene Geräte dieser Liste hinzugefügt.

Wenn die Geräteerkennung ein Gerät findet, versucht sie, den Gerätetyp zu ermitteln, damit sie das Gerät einer der folgenden Kategorien zuordnen kann:

- **Gehäuse:** Enthält Blade-Server Chassis Management Module (CMMs).
- **Computer:** Umfasst Computer. Linux-Systeme werden möglicherweise als Unix-Systeme in der Spalte **Betriebssystemname** ausgewiesen.
- **Infrastruktur:** Umfasst Router und andere Netzwerk-Hardware.
- **Intel AMT:** Enthält Geräte mit Unterstützung für Intel* Active Management Technology.
- **IPMI:** Enthält IPMI-taugliche Geräte.
- **Andere:** Umfasst nicht identifizierte Geräte.
- **Drucker:** Umfasst Drucker.

Dank dieser Kategorien bleibt die Liste **Geräteerkennung** übersichtlich. Auf diese Weise lassen sich die Geräte, für die Sie sich interessieren, leichter finden. Sie können die Geräteliste nach einer der Spaltenüberschriften sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Die Geräteerkennung ordnet die Geräte möglicherweise nicht immer richtig zu. Falsch eingeordnete Geräte lassen sich einfach in die richtige Gruppe verschieben, indem Sie auf **Verschieben** klicken, die richtige Kategorie auswählen und dann auf **OK** klicken.

Manchmal wird der Core Server zweimal aufgelistet. Dies geschieht, wenn dasselbe Gerät über einen anderen Erkennungsmechanismus (z. B. CBA, IPMI, CMM, PDS1 und PDS2) gefunden wurde und die Informationen des Geräts unter diesem Mechanismus der Datenbank hinzugefügt werden.

Nachdem Sie Agenten auf einem erkannten Gerät installiert haben und das Gerät einen Inventarscan an den Core gesendet hat, wird das erkannte Gerät aus der Liste mit den erkannten Geräten entfernt.

Filtern der Geräteliste

Suchen Sie mithilfe des Symbolleistenfelds **Filtern nach** nach Geräten, die mit den von Ihnen angegebenen Suchkriterien übereinstimmen. Sie können nach Knotenname, IP-Adresse, Subnetzmaske, Kategorie oder Betriebssystemname filtern. Bei Verwendung eines Filters werden Geräte alphabetisch nach dem Filterattribut gefiltert.

So filtern Sie die Geräteliste

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Klicken Sie in der Strukturansicht **Nicht verwaltete** auf die Gruppe, die Sie filtern möchten.
3. Klicken Sie im Feld **Filtern nach** auf das Attribut, das Sie als Filter setzen möchten. (Wenn **Filtern nach** nicht angezeigt wird, klicken Sie auf **>>**, um die Anzeige zu erweitern.)
4. Geben Sie in das neben dem Attribut zu sehende Feld den Text ein, den Sie als Filter verwenden möchten.
5. Klicken Sie auf **Suchen**.

Hinzufügen von Kategorien

Sie können Gerätekategorien erstellen, um nicht verwaltete Geräte zu gruppieren. Wenn Sie ein Gerät in eine andere Kategorie verschieben, wird es bei einer späteren Erkennung durch die Geräteerkennung wieder in dieser Gruppe angezeigt. Geräte, von denen Sie wissen, dass Sie sie nicht mit der Konsole verwalten werden, sollten in andere Gruppen verschoben werden, damit neue Geräte in der Gruppe**Computer** leichter erkennbar sind.

Wenn Sie eine Gruppe löschen, die Geräte enthält, werden diese Geräte von der Geräteerkennung in die Gruppe **Andere** verschoben.

So fügen Sie eine Gerätekategorie hinzu

1. Klicken Sie in der Ansicht **Geräte erkennen** auf **Kategorie hinzufügen**.
2. Geben Sie einen Namen für die Gruppe in das Feld **Kategoriename** ein und klicken Sie dann auf **OK**.
3. Um eine Kategorie, die Sie hinzugefügt haben, zu löschen, klicken Sie auf **Kategorie löschen** und klicken dann auf **OK**, um die Löschung zu bestätigen.

Verschieben von erkannten Geräten in die Liste "Eigene Geräte"

Nachdem Sie Geräte erkannt haben, können Sie sie in die Liste **Eigene Geräte** verschieben. Beim Verschieben der Geräte werden ihre zugehörigen Informationen der Datenbank hinzugefügt. Sobald die Informationen in die Datenbank geschrieben wurden, können Sie die Agentenkonfiguration bereitstellen, Abfragen und Berichte für diese Informationen ausführen sowie zahlreiche andere Verwaltungsaufgaben erledigen.

Bei Geräten, die Out-of-Band verwaltetet werden können (d. h. Geräte mit IPMI-, Intel AMT- oder DRAC-Funktionalität), haben Sie außerdem die Option zur Verwaltung, ohne einen Agenten bereitzustellen. Wenn Sie sich für diese Option entscheiden, werden die Geräteinformationen in der Datenbank und dem BMC des Geräts gespeichert, damit Sie die Verwaltungsfunktionen verwenden können, die von der Out-of-Band-Verwaltungshardware des Geräts unterstützt werden.

So verschieben Sie erkannte Geräte in die Liste "Eigene Geräte"

1. Klicken Sie in der Ansicht **Geräteerkennung** auf das Gerät, das Sie in die Liste **Eigene Geräte** verschieben möchten. Mit UMSCHALT+Mausklick oder STRG+Mausklicken können Sie mehrere Geräte auswählen.
2. Klicken Sie auf die Schaltfläche **Ziel**. Die ausgewählten Geräte werden dann unter der Registerkarte **Zielliste** aufgeführt.
3. Klicken Sie auf die Registerkarte **Verwalten**.
4. Wählen Sie **Zielgeräte verschieben** aus.
5. Wenn die Geräte Out-of-Band-Verwaltung unterstützen und Sie keinen Verwaltungsagenten auf den Geräten bereitstellen möchten, wählen Sie **Out-of-Band-kompatibles Gerät ohne Agent verwalten** aus.
6. Klicken Sie auf **Verschieben**.

Die Geräte werden aus der Liste der nicht verwalteten Geräten entfernt und in der Liste **Eigene Geräte** angezeigt.

Wenn Sie die Option für die Out-of-Band-Verwaltung ausgewählt haben, können Sie den Status des Verschiebevorgangs anzeigen, indem Sie auf die Registerkarte **Verschiebungsstatus** im unteren Fensterbereich klicken. Etwaige Fehler in der Konfiguration werden hier vermerkt. Um ein IPMI-taugliches Gerät in die Liste **Eigene Geräte** zu verschieben, müssen Sie die erforderlichen BMC-Anmeldeinformationen im Dienstprogramm Dienste konfigurieren bereitstellen, um dem Core Server die erfolgreiche Authentifizierung gegenüber dem Gerät zu ermöglichen.

Wenn Sie ein Chassis Management Module (CMM) in die Liste **Eigene Geräte** verschieben, wird es in der Liste **Alle Geräte** und zusätzlich als Gruppe in der Liste **Öffentliche Gruppen** angezeigt. Die Gruppendetails zeigen das CMM und eine Liste der verfügbaren Einschübe in dem betreffenden Gehäuse an, einschließlich der Namen der Blade-Server in diesen Einschüben. Die Blade-Server werden ebenfalls erkannt und als individuelle Server verwaltet.

Erkennen von Intel* AMT-Geräten

System Manager beinhaltet eine Option zum Erkennen von Geräten, die mit Intel* Active Management Technology (Intel* AMT) Version 1 konfiguriert wurden. Geräte können nur als Intel AMT-Geräte erkannt werden, nachdem Sie den Intel AMT-Konfigurationsbildschirm geöffnet und das Standardkennwort des Herstellers in ein starkes Kennwort geändert haben. (Weitere Informationen über den Zugriff auf den Intel AMT-Konfigurationsbildschirm finden Sie in der Dokumentation des Herstellers.) Wenn Sie diesen Schritt nicht ausgeführt haben, werden die Geräte zwar erkannt, jedoch nicht als Intel AMT-Geräte identifiziert; darüber hinaus wird nicht dieselbe Inventarübersicht angezeigt, die andernfalls angezeigt würde.

Geräte mit Intel AMT, Version 2, werden durch diesen diesen Prozess nicht erkannt. Nachdem Bereitstellungsgkennungen in den Intel AMT-Konfigurationsbildschirm mit der IP-Adresse des Core Serves eingegeben wurde, wird das Gerät automatisch erkannt. Weitere Informationen zur Verwendung von Version 2 finden Sie unter Konfigurieren von Intel AMT-Geräten.

So erkennen Sie Intel® AMT-Geräte

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Klicken Sie auf **Neu**, um eine neue Konfiguration zu erstellen, und geben Sie einen Namen für die Konfiguration ein. Oder klicken Sie auf eine vorhandene Konfiguration und klicken Sie auf **Bearbeiten**, um sie zu ändern.
3. Aktivieren Sie **Intel AMT-Geräte erkennen**.
4. Geben Sie Start- und Abschluss-IP-Adressen ein, um einen bestimmten Adressbereich zu scannen, und geben Sie eine Subnetzmaske ein.
5. Klicken Sie auf **Hinzufügen** und klicken Sie dann auf **OK**.
6. Wählen Sie die Konfiguration aus und klicken Sie dann auf **Planen**. Legen Sie Zeitplanoptionen fest oder klicken Sie auf **Jetzt starten** und dann auf **Speichern**.
7. Um den Fortschritt des Scanvorgangs anzuzeigen, klicken Sie auf die Registerkarte **Erkennungstasks**.

Für Intel AMT konfigurierte Geräte werden im Ordner **Intel AMT** angezeigt. Von diesem Ordner aus können Sie das Gerät auswählen und in die Liste der verwalteten Geräte einfügen.

Um das Gerät der Core-Datenbank hinzuzufügen (damit es verwaltet werden kann), müssen Benutzername/Kennwort für das Gerät mit dem Benutzernamen/Kennwort übereinstimmen, der/das im Dienstprogramm "Dienste konfigurieren" gespeichert wurde. Dieser Vorgang ermöglicht System Manager die Authentifizierung gegenüber dem Gerät. Wenn Sie die Kennwortkonfiguration im Dienstprogramm "Dienste konfigurieren" speichern, so werden die Informationen in der Core-Datenbank gespeichert, damit System Manager gegenüber Intel AMT-Geräten authentifiziert werden kann.

Bei Intel AMT-Geräten mit unterschiedlichen Anmeldeinformationen müssen Sie sicherstellen, dass die Anmeldeinformationen für das jeweilige Gerät mit denen im Dienstprogramm "Dienste konfigurieren" übereinstimmen, da Sie die Geräte andernfalls nicht verwalten können.

Wenn ein Intel AMT-Gerät erkannt und in die Liste **Eigene Geräte** verschoben wird, erfolgt seine Provisionierung automatisch unter Verwendung des Modus, den Sie im Dienstprogramm "Dienste konfigurieren" auswählen. Der Small Business-Modus bietet einfache Verwaltungsfunktionen ohne Netzwerkinfrastrukturdienste (Sicherheitsmodus 1), während der Enterprise-Modus für große Unternehmen vorgesehen ist. Dieser Modus bietet Sicherheit auf der Basis von Netzwerkdiensten wie DHCP, DNS und einem TLS-Zertifikatsautoritätsdienst.

Wenn Ihr Core mit einem Proxy-Server arbeitet, muss der Proxy-Server "Digest Access-Authentifizierung" unterstützen, um Intel AMT-Geräte erkennen zu können.

So konfigurieren Sie das Intel AMT-Kennwort

1. Klicken Sie auf **Start | Alle Programme | LANDesk | Dienste konfigurieren**. Klicken Sie auf die Registerkarte **Intel AMT-Konfiguration**.

2. Geben Sie den aktuellen Benutzernamen und das aktuelle Kennwort ein. Um Intel AMT-Geräte verwalten zu können, müssen Benutzername und Kennwort mit dem im Intel AMT-Konfigurationsbildschirm konfigurierten Benutzernamen und Kennwort übereinstimmen (auf diesen Bildschirm wird über die BIOS-Einstellungen des Computers zugegriffen).
3. Um den Benutzernamen und das Kennwort zu ändern, füllen Sie den Abschnitt **Neues Intel AMT-Kennwort** aus.
4. Wählen Sie den Modus (**Small Business** oder **Enterprise**) aus, den Sie für die Provisionierung von Geräten verwenden möchten, wenn Sie die Geräte (um sie zu verwalten) der Core-Datenbank hinzufügen.
5. Klicken Sie auf **OK**. Diese Änderung wird vorgenommen, wenn die Clientkonfiguration ausgeführt wird.

So verschieben Sie erkannte Intel AMT-Geräte in die Liste der verwalteten Geräte

1. Klicken Sie auf mindestens einen Gerätenamen in der Liste der nicht verwalteten Geräte.
2. Klicken Sie auf die Schaltfläche **Ziel** in der Symbolleiste.
3. Klicken Sie auf die Schaltfläche **Verwalten** im unteren Fensterbereich, wählen Sie **Zielgeräte verschieben** aus und klicken Sie dann auf **Verschieben**.

   Wenn alle Geräte, die Sie verwalten möchten, in der Liste angezeigt werden, können Sie sie auswählen, auf die Schaltfläche **Verwalten** im unteren Fensterbereich klicken, **Ausgewählte Geräte verschieben** auswählen und dann auf **Verschieben** klicken.

Das Gerät wird aus der Liste mit den nicht verwalteten Geräten entfernt und in die Liste **Alle Geräte** eingefügt. Beachten Sie, dass die Intel AMT-Provisionierung beim Verschieben von Geräten in die Liste **Eigene Geräte** in einem separaten Hintergrundprozess ausgeführt wird. Sie können - während dieser Vorgang ausgeführt wird - andere Erkennungs- oder Verwaltungsaufgaben ausführen.

Weitere Informationen zum Verwalten von Intel AMT-Geräten finden Sie unter Verwalten von Intel* AMT-Geräten und Intel* AMT-Support.

Installation und Konfiguration von Geräteagenten

Übersicht über die Installation und Konfiguration von Agenten

Um Geräte komplett über die Konsole verwalten zu können, müssen Sie Verwaltungsagenten auf den Geräten installieren. Sie können die Standard-Agentenkonfiguration installieren (installiert alle Produktagenten), oder Sie können eigene Agentenkonfigurationen anpassen, um sie auf Ihren Geräten zu installieren. Bei der Installation von System Manager werden keine Agenten automatisch auf dem Core installiert; die Agenten müssen von Ihnen auf dem Core installiert und der Core muss dann manuell neu gestartet werden. Die Agentenkonfiguration muss den Überwachungsagenten für den Empfang von Warnmeldungen zum Systemzustand enthalten.

Verwaltungsagenten können mit einem der folgenden Verfahren installiert werden:

- Verteilen von Agenten Wählen Sie in der Liste **Eigene Geräte** Zielgeräte aus und planen Sie dann einen Konfigurationstask für Agenten, um Agenten über eine Fernsteuerungsverbindung auf den Geräten zu installieren.
- Installieren von Agenten mit einem Installationspaket Erstellen Sie ein selbstextrahierendes Geräteinstallationspaket. Führen Sie dieses Paket lokal auf dem Gerät aus, um die Agenten zu installieren. Während dieses Vorgangs müssen Sie mit Administratorrechten angemeldet sein.
- Herunterladen des Agenten mit einer Pull-Prozedur Definieren Sie eine Zuordnung zur ldlogon-Freigabe des Cores (//*servername*/ldlogon) und führen Sie SERVERCONFIG.EXE aus.
- Manuell auf einem Gerät mit einem mobilen USB-Laufwerk (weitere Informationen erhalten Sie unter Installieren von Agenten mit einem Installationspaket)

Eine weitere Informationsquelle für die Installation und Konfiguration von Agenten ist das Kapitel Geräteerkennung im *Benutzerhandbuch*.

Hinweis: Sie können eine Gerätekonfiguration zur Standardkonfiguration machen, indem Sie die Konfiguration auf der Seite **Agentenkonfiguration** auswählen und dann auf **Als Standard festlegen** klicken. Eine reine IPMI BMC-Konfiguration kann nicht als Standardkonfiguration ausgewählt werden. Standardkonfigurationen können nicht gelöscht werden.

Unter Windows muss die Firewall für die folgenden Anschlusseinstellungen manuell konfiguriert werden, um alle Funktionen des Produkts nutzen zu können. Greifen Sie über die Systemsteuerung auf die Windows-Firewall zu, um diese Einstellungen zu ändern.

Verwaltete Server:

- Datei- und Druckerfreigabe: TCP 139, 445; UDP 137,138 (unabdingbare Voraussetzung für den Push-Prozess)
- Softwareverteilung: TCP 9595 (unabdingbare Voraussetzung für den Push-Prozess)

- Erweitert: ICMP - "Allow incoming echo request" (Kann nicht erkannt werden, wenn diese Einstellung nicht aktiviert ist.)

Core Server:

- Inventar: 5007
- Fernsteuerung: 9535

Klicken Sie hierfür auf **Start** | **Systemsteuerung** | **Sicherheit**.

Aktualisieren vorhandener Agenten

Sie können Agentenkonfigurationen mit einer Push-Prozedur auf Ihre Geräte übertragen, selbst wenn die Standard Management- oder Fernsteuerungsagenten noch nicht installiert sind. Weitere Informationen zum Konfigurieren von Anmeldeinformationen finden Sie unter Konfigurieren von Diensten und Anmeldeinformationen im *Benutzerhandbuch*.

Nachdem Sie ein Agentenpaket installiert haben, wird bei der Installation die vorherige Installation entfernt und die neue installiert. Sie können einen Agenten deinstallieren, indem Sie ein neues Agentenpaket erstellen, das den Agenten, der entfernt werden soll, nicht einschließt.

Deinstallieren von Agenten

Führen Sie den folgenden Vorgang aus, um Agenten auf Servern zu deinstallieren.

Warnung: Das Gerät wird von "Uninstallwinclient.exe" nach dem Deinstallieren der Agenten standardmäßig neu gestartet, es sei denn, Sie verwenden den Schalter **/noreboot** in der Befehlszeile. Der Neustart ist erforderlich, um die Deinstallation abzuschließen. Beim Initiieren eines Neustarts wird der Server ohne Warnung neu gestartet und die Schließung aller anderen Anwendungen erzwungen. Der /noreboot-Schalter lässt den Server weiterarbeiten, ohne dass ein Neustart ausgeführt wird.

So deinstallieren Sie Agenten auf einem Server

1. Melden Sie sich mit administrativen Rechten am Server an.
2. Ordnen Sie der Freigabe **ldmain** des Core Servers ein Laufwerk zu.
3. Öffnen Sie eine Befehlsaufforderung, wechseln Sie zum Laufwerksbuchstaben des Ordners "ldmain" und geben Sie Folgendes ein:

   ```
   uninstallwinclient.exe /noreboot
   ```

Die Deinstallation wird im Hintergrund ausgeführt und löscht alle Agenten.

Sie können auch **Start** > **Ausführen** >***Core Name*\ldmain\uninstallwinclient.exe /noreboot** auswählen.

So deinstallieren Sie Agenten auf einem Linux-Server

1. Kopieren Sie die Datei "linuxuninstall.tar.gz" auf das Linux-Gerät in ein temporäres Verzeichnis. Die Datei befindet sich im freigegebenen ManagementSuite-Ordner auf dem Core Server.

   Möglicherweise ist Samba auf dem Linux-Gerät nicht installiert/konfiguriert, sodass ein direktes Kopieren nicht möglicht ist; Sie können sie jedoch ggf. mit "pscp" vom Core laden, in den Ordner "ldlogon" oder auf einen austauschbaren Datenträger kopieren.
2. Dekomprimieren Sie diese Datei an einer Shell-Eingabeaufforderung (auf dem Linux-Rechner); verwenden Sie hierfür tar und die Optionen x, z und f.

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. Nachdem die Datei dekomprimiert wurde, führen Sie von einer Shell-Eingabeaufforderung im aktuellen Verzeichnis das "linuxuninstall"-Skript aus.

   ```
   ./linuxuninstall.sh
   ```

Konfigurieren von Agenten

Um Geräte komplett über die Konsole verwalten zu können, müssen Verwaltungsagenten auf den Geräten installiert sein. Die Installation von System Manager schließt nicht das automatische Installieren von Agenten auf dem Core ein. Die Agenten müssen von Ihnen auf dem Core installiert werden und anschließend müssen Sie den Core manuell neu starten. Unabhängig davon, ob Sie eine der Standardkonfigurationen für Agenten verwenden oder eine Agentenkonfiguration in der Konsole erstellen, können Sie die Konfiguration auf drei Arten auf Windows- oder Linux-Geräten installieren:

- Erstellen Sie eine Agentenkonfiguration, wählen Sie Geräte in der Liste **Eigene Geräte** als Ziel aus und planen Sie dann einen Konfigurationstask für Agenten, um Agenten remote auf den Geräten zu installieren.
- Erstellen Sie ein selbstextrahierendes Installationspaket. Führen Sie dieses Paket lokal auf dem Gerät aus, um die Agenten zu installieren. Während dieses Vorgangs müssen Sie mit Administratorrechten angemeldet sein. Weitere Informationen finden Sie unter Installieren von Agenten mit einem Installationspaket.
- Konfigurieren Sie von einem Windows-Gerät aus eine Zuordnung zur Freigabe "ldlogon" des Cores (*myserver*\ldlogon) und führen Sie SERVERCONFIG.EXE aus.

So erstellen Sie eine Agentenkonfiguration

1. Klicken Sie im linken Navigationsfenster auf **Agentenkonfiguration**.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Namen für die neue Konfiguration in das Feld **Konfigurationsname** ein.

   Geben Sie einen Namen ein, der die Konfiguration beschreibt, an der Sie arbeiten. Dies kann ein bereits vorhandener oder ein neuer Konfigurationsname sein.

4. Wählen Sie die Plattform für die Konfiguration aus.

5. Wählen Sie den Installationstyp der Konfiguration aus (vom "Benutzer ausgewählt" oder "IPMI Nur BMC"). Wählen Sie **IPMI Nur BMC** unter **Konfiguration** aus, um den Baseboard Management Controller (BMC) auf IPMI-tauglichen Geräten auszuwählen (siehe Hinweis unter Schritt 9 weiter unten).

   Eine Konfiguration vom Typ "IPMI Nur BMC" konfiguriert den Baseboard Management Controller für Out-of-Band-Zugriff, führt einen vollständigen Inventarscan aus und veranlasst, dass die Konfiguration sich selbst löscht. Eine reine IPMI BMC-Konfiguration kann nicht als Standardkonfiguration ausgewählt werden. Hinweis: Wenn Sie eine Konfiguration vom Typ "IPMI Nur BMC" erstellen, stehen die meisten in den folgenden Schritten beschriebenen Bearbeitungsoptionen nicht zur Verfügung.

6. Wählen Sie die Konfiguration aus, die Sie soeben erstellt haben, und klicken Sie auf **Bearbeiten**.

   Auf den Registerkarten sind einige Optionen abgeblendet, da sie für die von Ihnen ausgewählte Konfiguration nicht konfigurierbar sind.
7. Wählen Sie auf der Registerkarte **Agent** die Agenten aus, die Sie bereitstellen möchten.

   - **Alle:** Installiert alle Agenten auf dem ausgewählten Gerät.
   - **Standard-Verwaltungsagent:** Bildet die Grundlage für die Kommunikation zwischen den Geräten und dem Core Server. Dies ist ein erforderlicher Agent (ausgenommen für Konfigurationen vom Typ "Nur BMC"). Die meisten Prozesse dieses Agenten sind bedarfsgesteuert.
   - **Software-Updates:** Installiert den Software-Updates-Scanners. Wenn dieser Agent installiert ist, können Sie festlegen, wie der Scanner ausgeführt wird. Dies ist kein bedarfsgesteuerter Agent.
   - **Überwachung:** Installiert den Überwachungsagenten auf dem ausgewählten Server. Der Überwachungsagent unterstützt zahlreiche Überwachungsmethoden, einschließlich Direct ASIC-Überwachung, In-Band-IPMI, Out-of-Band-IPMI und CIM. Dies ist kein bedarfsgesteuerter Agent.
   - **Active System Console:** Installiert den Agenten, der es ermöglicht, dass von System Manager aus über die Benutzeroberfläche oder die Menüs auf die Active System Console zugegriffen werden kann. Dieser Agent wird nur auf Geräten mit Intel-Platinen unterstützt.

8. Wählen Sie unter **Konfiguration** für die Systemtypfelder den Typ aus. Wenn diese Optionen abgeblendet sind, bedeutet dies, dass Sie den Typ bereits ausgewählt haben.

9. Wählen Sie eine Option für den **Neustart** aus.

   Manuell neu starten bedeutet, dass Geräte nach der Installation nicht automatisch neu gestartet werden. Nach einer Agentenkonfiguration muss kein Neustart des Geräts ausgeführt werden. Das Gerät muss von Ihnen manuell neu gestartet werden.

   Beim Neustarten wird, falls erforderlich, ein Neustart für Agenten-Updates ausgeführt, wenn aktualisierte Dateien gesperrt sind.

10. Definieren Sie auf der Registerkarte Inventar die Konfigurationseinstellungen für den Inventarscanner. Diese Optionen werden nachstehend erläutert.

- **Automatische Aktualisierung:** Remote-Geräte lesen die Softwareliste des Core Servers während des Softwarescans. Wenn diese Option ausgewählt ist, muss jedes Gerät über ein Laufwerk verfügen, das dem Verzeichnis LDLOGON auf dem Core Server zugewiesen wurde, damit es auf die Softwareliste zugreifen kann. In der Softwareliste erfolgte Änderungen stehen den Geräten sofort zur Verfügung.
- **Manuelle Aktualisierung:** Die während der Softwarescans zum Ausschließen von Titeln verwendete Softwareliste wird in jedes Remote-Gerät geladen. Immer, wenn die Softwareliste von der Konsole aus geändert wird, müssen Sie sie manuell erneut an die Remote-Geräte weiterleiten.
- **Inventarscanner-Einstellungen:**Der Zeitpunkt, zu dem die Inventarisierung ausgeführt wird. Sie können die Häufigkeit auswählen und Sie können angeben, dass der Inventarscanner bei jedem Systemstart ausgeführt werden soll. Sie können den Scanner manuell vom verwalteten Server über Start **|** Programme **|** LANDesk Management **|** Inventarscan ausführen. In Linux sollten Sie als Root angemeldet sein und folgende Anweisung von der Befehlsziele aus ausführen: `/usr/LANDesk/ldms/ldiscan -ntt`

    - **Auszuführen bei der Anmeldung:** Der Inventarscanner wird beim Gerätestart ausgeführt. Wenn Sie eine HP-UX-Konfiguration erstellen, ist diese Schaltfläche abgeblendet, da der HP-UX-Scanner als cron-Auftrag eingerichtet ist, der entweder täglich, wöchentlich oder monatlich läuft. Dies kann nicht geändert werden.
    - **Startzeit:** Geben Sie an, innerhalb von welchem Stundenzeitraum der Scanner ausgeführt werden kann. Meldet sich ein Gerät während des angegebenen Zeitraums an, so wird automatisch der Inventarscanner ausgeführt. Wenn das Gerät bereits angemeldet ist, wird der Scan zur angegebenen Stunde automatisch gestartet. Diese Option ist nützlich, wenn Sie Inventarscans auf Geräten zeitlich versetzt ausführen möchten, um zu verhindern, dass alle Scans gleichzeitig gesendet werden.
    - **Wiederholen alle:** Geben Sie eine Zahl ein, die dem Inkrement (z. B. 1, 2 oder 3) und der Zeiteinheit (Minuten, Stunden oder Tage) entspricht.
    - **Beschränkungen:** Legt fest, an welchen Tagen und zu welcher Uhrzeit der Scanner ausgeführt werden darf. Klicken Sie auf **Tageszeit**, **Wochentag** oder **Tag des Monats** und geben Sie einschließende Parameter ein. Geben Sie z. B. 10 für **Tag des Monats** und 1:00 Uhr und 3:00 Uhr für **Tageszeit**, um zu veranlassen, dass der Inventarscanner am 10. eines jeden Monats zwischen 1:00 Uhr und 3:00 Uhr ausgeführt wird.

11. Legen Sie auf der Registerkarte **Software-Updates** die Tage und die Uhrzeit für die Ausführung des Software-Updates-Scanner fest. Der Scanner wird automatisch ausgeführt, ohne dass ein geplanter Task erstellt werden muss.
    - **Auszuführen bei der Anmeldung:** Der Software-Updates-Scanner wird beim Starten des Geräts ausgeführt.
    - **Startzeit:** Geben Sie an, innerhalb von welchem Stundenzeitraum der Scanner ausgeführt werden kann. Meldet sich ein Gerät während des angegebenen Zeitraums an, so wird automatisch der Software-Updates-Scanner ausgeführt. Wenn das Gerät bereits angemeldet ist, wird der Software-Updates-Scan zur angegebenen Stunde automatisch gestartet. Diese Option ist nützlich, wenn Sie Scans auf Geräten zeitlich versetzt ausführen möchten, um zu verhindern, dass alle Scans gleichzeitig gesendet werden.

- **Wiederholen alle:** Geben Sie eine Zahl ein, die dem Inkrement (z. B. 1, 2 oder 3) und der Zeiteinheit (Minuten, Stunden oder Tage) entspricht.
- **Beschränkungen:** Legt fest, an welchen Tagen und zu welcher Uhrzeit der Software-Updates-Scanner ausgeführt werden darf. Klicken Sie auf **Tageszeit**, **Wochentag** oder **Tag des Monats** und geben Sie einschließende Parameter ein. Geben Sie z. B. 10 für **Tag des Monats** und 1:00 Uhr und 3:00 Uhr für **Tageszeit** ein, um zu veranlassen, dass der Inventarscanner am 10. eines jeden Monats zwischen 1:00 Uhr und 3:00 Uhr ausgeführt wird.

12. Wählen Sie auf der Registerkarte **Regelsätze** einen Überwachungs- und/oder Alarmregelsatz aus, den Sie in die Konfiguration einfügen möchten. Diese Regelsätze werden im Ordner "ldlogon/alertrules" gespeichert. Neue Regelsätze können in **Überwachung**oder **Alarmierung** erstellt werden. Damit neu erstellte Regelsätze in den Dropdown-Listen angezeigt werden, müssen Sie die XML für den benutzerdefinierten Regelsatz generieren.
13. Klicken Sie auf **Änderungen speichern**, um die Informationen in der Datenbank zu speichern. Klicken Sie auf **Speichern als Datei**, um die Konfiguration als ein Verteilungspaket zu speichern.

Hinweis: Sie können eine Agentenkonfiguration zur Standardkonfiguration machen, indem Sie die Konfiguration auf der Seite **Agentenkonfiguration** auswählen und dann auf **Als Standard festlegen** klicken. Standardkonfigurationen können nicht gelöscht werden.

So planen Sie einen Agentenkonfigurationstask

1. Klicken Sie im linken Navigationsfenster auf **Agentenkonfiguration**.
2. Klicken Sie auf die Agentenkonfiguration und dann auf **Task planen**.
3. Bearbeiten Sie die Liste mit den Zielgeräten und den Taskzeitplan.
4. Klicken Sie auf **Speichern**.

Wenn Sie auf **Task planen** klicken, wird ein Task erstellt (er verfügt über keine Zielgeräte und keinen Zeitplan). Wenn Sie diesen Agentenkonfigurationstask abbrechen, ohne ihn zu speichern, gilt der Task dennoch als erstellt und wird in der **Taskliste** mit dem Status "Nicht geplant" angezeigt. Sie können den Task aus der Liste **Eigene Tasks** löschen.

Nachdem der Agentenkonfigurationstask abgeschlossen ist, müssen Sie das Gerät neu starten, um Details zum Gerät in der Konsole anzuzeigen (siehe Anzeigen der Serverinformationskonsole). Ganz gleich, ob Sie den Agenten auf dem Core Server oder auf verwalteten Geräten installieren, müssen Sie in beiden Fällen einen Neustart ausführen. Mithilfe des Agentenkonfigurationsprozesses können Sie festlegen, wann der Neustart auszuführen ist (um eine Beeinträchtigung der Servernutzung zu verhindern).

Bereitstellen von Agenten auf verwalteten Geräten

Sobald Geräte erkannt wurden, können Agenten auf diesen Geräten bereitgestellt werden. Agenten können nur auf unterstützten Windows-, Linux- und HP-UX-Geräten bereitgestellt werden. Zum Bereitstellen von Agenten auf Windows-Geräten benötigen Sie Administratorrechte und zum Konfigurieren von Linux- und HP-UX-Geräten benötigen Sie das Stammrecht.

Es gibt folgende Möglichkeiten, Agenten auf nicht verwalteten Geräten bereitzustellen:

- Über Push-basierte Bereitstellungen mithilfe eines Erkennungsauftrags und eines Domänenverwaltungskontos, das Sie für den Scheduler-Dienst, der Erkennungsaufträge verarbeitet, konfiguriert haben. Das Domänenverwaltungskonto erteilt den Scheduler-Diensten die für die Installation der Serveragenten erforderlichen Rechte. Dies funktioniert für Server der Windows NT-Produktfamilie.
- Über Push-basierte Bereitstellungen mithilfe des Standard Management Agent. Wenn die Server über den Standard Management Agent verfügen, der von vielen LANDesk Software-Produkten verwendet wird, können Sie Bereitstellungen auf den Servern durchführen, ohne dass Sie ein Domänen-Verwaltungskonto benötigen.

Verwenden Sie beim Bereitstellen auf erkannten Geräten die Option **Filtern nach** der Strukturansicht **Nicht verwaltet**. Sie können nach der IP-Adresse filtern, um Geräte zu isolieren.

Für Windows-Systeme setzen die folgenden Anschlusseinstellungen voraus, dass die Firewall manuell konfiguriert wurde, um alle Funktionen des Produkts nutzen zu können. Greifen Sie über die Systemsteuerung auf die Windows-Firewall zu, um diese Einstellungen zu ändern.

Verwaltete Server:

- Datei- und Druckerfreigabe: TCP 139, 445; UDP 137,138 (unabdingbare Voraussetzung für den Push-Prozess)
- Softwareverteilung: TCP 9594, 9595 (unabdingbare Voraussetzung für den Push-Prozess)
- Erweitert - ICMP: "Allow incoming echo request" (Kann nicht erkannt werden, wenn diese Einstellung nicht aktiviert ist.)

Core Server:

- Inventar: 5007
- Fernsteuerung: 9535

Konfigurieren von Berechtigungsnachweisen für die Geräteauthentifizierung

Nicht verwaltete Geräte, auf denen der Standard Management Agent installiert ist, benötigten keine Berechtigungsnachweise zur Authentifizierung für die Agentenbereitstellung. Um Agenten auf Windows-Geräten zu installieren, die nicht über den Standard Management Agent verfügen, müssen Sie die Berechtigungsnachweise angeben, die der Scheduler-Dienst auf der Konsole verwenden wird, um die erforderlichen Rechte zu erhalten.

Um Geräteagenten auf nicht verwalteten Geräten zu installieren, muss der Scheduler-Dienst in der Lage sein, mit einem administrativen Konto Verbindungen zu Geräten herzustellen. LocalSystem ist das vom Scheduler-Dienst verwendete Standardkonto. Die LocalSystem-Berechtigungsnachweise funktionieren im Allgemeinen für Geräte, die sich nicht in der Domäne befinden.

Bei Geräten, die sich in einer Domäne befinden, müssen Sie ein Domänenadministrator-Konto angeben. Wenn Sie nicht verwaltete Geräte in mehreren Domänen konfigurieren, müssen Sie diese Geräte Domäne für Domäne konfigurieren, da der Scheduler-Dienst für die

Authentifizierung nur einen Satz Berechtigungsnachweise verwendet und für jede Domäne ein anderes Domänenverwaltungskonto benötigt wird.

Mit dem Hilfsprogramm "Dienste konfigurieren", das zum Core Server gehört, können Inventaroptionen angepasst werden. Dieses Programm kann nur auf dem Core Server ausgeführt werden.

So konfigurieren Sie die Berechtigungsnachweise für die Anmeldung für den Scheduler-Dienst

1. Starten Sie das Hilfsprogramm "Dienste konfigurieren" auf dem Core Server, indem Sie auf **Start | Programme | LANDesk | Dienste konfigurieren** klicken.
2. Klicken Sie auf die Registerkarte **Scheduler**.
3. Klicken Sie auf **Anmeldung ändern**.
4. Geben Sie die Berechtigungsnachweise ein, die der Dienst auf Clients verwenden soll, für gewöhnlich ein Domänenadministratorkonto.

Installieren von Agenten

Sobald Sie eine Agentenkonfiguration in der Konsole erstellt haben, können Sie sie auf Geräten installieren. Bei der Installation von System Manager werden keine Agenten automatisch auf dem Core installiert; die Agenten müssen von Ihnen auf dem Core installiert und der Core muss dann manuell neu gestartet werden.

Bei den Clientagent-Paketen handelt es sich um selbstextrahierende ausführbare Dateien. Standardmäßig werden Sie im Ordner "\Programme\LANDesk\ManagementSuite\ldlogon" auf dem Core Server gespeichert. Durch Starten der ausführbaren Datei werden die Clientagenten ohne Benutzerabfragen im Hintergrund installiert. Ein Browser auf dem Zielgerät ist keine Voraussetzung für eine erfolgreiche Agenteninstallation.

Installieren von Agenten

Sie können die Agenten aktualisieren, indem Sie eine neue Clientkonfiguration erstellen und von der Konsole aus verteilen; oder installieren Sie Agenten direkt auf nicht verwalteten Geräten.

Sobald Sie ein Clientagent-Paket installiert haben, werden beim Installieren weiterer Clientagent-Pakete alle Agenten entfernt und die speziell ausgewählten Agenten installiert. Sie können einen Agenten deinstallieren, indem Sie ein neues Clientagent-Paket erstellen, das den zu entfernenden Agenten nicht einschließt.

Deinstallieren von Agenten

Wenn Sie Agenten auf Geräten deinstallieren müssen, lesen Sie die Informationen unter Übersicht zur Installation und Konfiguration von Agenten.

Installieren von Agenten mithilfe eines Installationspakets

Eine Möglichkeit, Agenten zu installieren, ist die Verwendung eines selbstextrahierenden Geräteagenten-Pakets. Damit können Sie die Datei auf ein CD- oder USB-Laufwerk kopieren und Agenten manuell installieren. Sie können diese Pakete erstellen, indem Sie auf **Als Datei speichern** im unteren Abschnitt des Dialogfelds **Konfiguration** klicken.

1. Klicken Sie auf **Agentenkonfiguration** und doppelklicken Sie dann auf einen Konfigurationsnamen.
2. Klicken Sie im Dialogfeld **Agentenkonfiguration** auf **Als Datei speichern** und klicken Sie dann auf **Schließen**.

Durch Klicken auf **Als Datei speichern** wird ein selbstextrahierendes ausführbares Paket mit einem Dateinamen erstellt, der mit dem von Ihnen angegebenen Konfigurationsnamen identisch ist. Es vergehen möglicherweise einige Minuten, bevor das Paket im Ordner "\Programme\LANDesk\ManagementSuite\ldlogon\ConfigPackages" auf dem Core Server zur Verfügung steht.

Durch Starten der ausführbaren Datei werden die Serveragenten ohne Benutzerabfragen im Hintergrund installiert. Sie müssen sich mit Administratorrechten anmelden, um das Paket zu installieren.

Wenn Ihre Benutzer sich nicht mit administrativen Rechten anmelden können, um das Paket zu installieren, können Sie die Pakete per E-Mail, Web-Download, Anmeldeskript oder über eine Freigabe bereitstellen.

Abrufen der Agenten mit einer Pull-Prozedur

Dieser Abschnitt enthält Hinweise zum Bereitstellen von Agenten von der Befehlszeile aus. Mit den SERVERCONFIG.EXE-Befehlszeilenparametern können Sie steuern, welche Komponenten auf den Geräten installiert werden. Sie können SERVERCONFIG.EXE im Standalone-Modus starten. Die Datei befindet sich in der Freigabe *http:\\coreserver\LDLogon*, die von jedem Windows-Server aus lesbar ist.

SERVERCONFIG.EXE verwendet zum Konfigurieren von Geräten SERVERCONFIG.INI.

Erläuterungen zur SERVERCONFIG.EXE

SERVERCONFIG.EXE konfiguriert Server der Windows NT-Produktfamilie mithilfe des folgenden Verfahrens für Verwaltungsaufgaben:

1. SERVERCONFIG bestimmt, ob der Computer zuvor schon einmal konfiguriert mit einem Verwaltungsagenten konfiguriert wurde. Wenn ja, entfernt SERVERCONFIG alle Komponenten und installiert ausgewählte Komponenten neu.

2. SERVERCONFIG lädt die geeignete Initialisierungsdatei (SERVERCONFIG.INI) und führt die darin enthaltenen Anweisungen aus.

Für SERVERCONFIG.EXE stehen folgende Befehlszeilenparameter zur Verfügung:

Parameter	Beschreibung
/I	Einzuschließende Komponenten (Anführungszeichen eingeschlossen): "Common Base Agent" "Inventarscanner" "Alarmierung" "Anfälligkeitsscanner" "Serverüberwachung" Sie können diese Komponenten auf einer Befehlszeile miteinander kombinieren. Beispiel: `SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner"`
/L oder /Log=	Pfad zu den CFG_YES- und CFG_NO-Protokolldateien, die aufzeichnen, welche Server konfiguriert wurden und welche nicht.
/LOGON	Ausführen [LOGON] von vordefinierten Befehlen
/N oder /NOUI	Keine Anzeige der Benutzeroberfläche
/NOREBOOT	Server nach Abschluss nicht neu starten (Standard)
/REBOOT	Erzwingen des Neustarts nach der Ausführung
/X=	Auszuschließende Komponenten. Beispiel: `SERVERCONFIG.EXE /X=SD`
/CONFIG= /[CONFIG]=	Spezifiziert eine Serverkonfigurationsdatei, die anstelle der SERVERCONFIG.INI-Dateien zu verwenden ist. Wenn Sie beispielsweise Konfigurationsdateien mit den Namen NTTEST.INI erstellt haben, verwenden Sie diese Syntax: `SERVERCONFIG.EXE /CONFIG=TEST.INI`

Parameter	Beschreibung
	Die benutzerdefinierten .INI-Dateien sollten sich im selben Verzeichnis wie SERVERCONFIG.EXE befinden. Beachten Sie auch, dass der Parameter /config den Dateinamen ohne das NT-Präfix verwendet.
/? oder /H	Anzeigen des Hilfemenüs

Erstellen einer Agentenkonfiguration

Verwenden Sie **Agentenkonfiguration** zum Erstellen und Aktualisieren von Agentenkonfigurationen (welche Agenten auf verwalteten Servern installiert werden etc.). Sie können verschiedene Konfigurationen erstellen, die auf den jeweiligen Bedarf spezifischer Gruppen zugeschnitten sind. Sie könnten beispielsweise eine Konfiguration für Webserver erstellen und eine andere für Anwendungsserver.

Um eine Konfiguration auf einen Server zu übertragen, müssen Sie folgende Schritte ausführen:

- **Die Agentenkonfiguration erstellen**: Definieren Sie spezifische Konfigurationen für Ihre Server.
- **Die Agentenkonfiguration planen**: Verteilen Sie die Konfiguration als Pull-Task an Server oder führen Sie vom Server aus SERVERCONFIG.EXE aus der LDLogon-Freigabe des Core Servers aus.

So erstellen Sie eine Agentenkonfiguration

1. Klicken Sie in der Konsole auf **Agentenkonfiguration**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neu**.
3. Geben Sie einen **Konfigurationsnamen** ein, wählen Sie das Betriebssystem aus und klicken Sie dann auf **OK**.
4. Klicken Sie auf den neuen Konfigurationsnamen und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie die Agenten aus, die Sie bereitstellen möchten.
6. Verwenden Sie die Registerkarten oben im Dialogfeld, um zu den Optionen zu navigieren, die sich auf die Komponenten beziehen, die Sie ausgewählt haben. Passen Sie die von Ihnen ausgewählten Optionen nach Bedarf an.
7. Klicken Sie auf **Änderungen speichern** und schließen Sie das Dialogfeld.
8. Wenn Sie die Konfiguration zum Standard festlegen möchten, wählen Sie **Als Standardkonfiguration festlegen**.

Abrufen einer Linux-Agentenkonfiguration mit einer Pull-Prozedur

So rufen Sie eine Linux-Agentenkonfiguration mit einer Pull-Prozedur ab

1. Erstellen Sie ein temporäres Verzeichnis auf dem Linux-Gerät (z. B. /tmp/ldcfg) und kopieren Sie Folgendes in das Verzeichnis:

   1. Alle Dateien aus dem Verzeichnis "LDLOGON\unix\linux".
   2. Das nach der Konfiguration benannte Shell-Skript (<*Konfigurationsname*>.sh) in das temporäre Verzeichnis.
   3. Kopieren Sie die nach der Konfiguration benannte *.0-Datei in das temporärer Verzeichnis. Das * repräsentiert acht Zeichen (0-9, a-f).
   4. Kopieren Sie alle in der Datei <*Konfigurationsname*>.ini aufgelisteten Dateien in das temporäre Verzeichnis. Um diese Dateien zu identifizieren, durchsuchen Sie die .INI-Datei nach "FILE*xx"*, wobei *xx* einer Zahl entspricht. Die Mehrzahl der Einträge, die Sie finden werden, wurden vom Client in Schritt 1 kopiert; Sie werden jedoch auch .XML-Dateien finden, die kopiert werden müssen. Die Dateinamen sollten, bis auf die folgenden Ausnahmen, nicht geändert werden:
      - alertrules\<*beliebiger Text*>.ruleset.xml sollte in internal.ruleset.xml umbenannt werden.
      - monitorrules\<*beliebiger Text*>.ruleset.monitor.xml sollte in masterconfig.ruleset.monitor.xml umbenannt werden

2. Wenn das Gerät über IPMI und einen BMC verfügt (mit in der Installation eingeschlossener Überwachung), geben Sie Folgendes in einer Befehlszeile ein:

   ```
   export BMCPW="(bmc password)"
   ```

3. Führen Sie (in einer Ausführung als Root) das Shell-Skript für die Konfiguration aus. Wenn Sie das Skript beispielsweise "pull" genannt haben, verwenden Sie den nachstehenden vollständigen Pfad:

   ```
   /tmp/ldcfg/pull.sh
   ```

4. Entfernen Sie das temporäre Verzeichnis einschließlich Inhalt.

Hinweis: Beachten Sie, dass beim Bereitstellen eines Agenten auf einem Linux-Gerät mittels Push- oder Pull-Vorgang, anschließendem Ausführen von

```
./linuxuninstall.sh -f ALL
```

zum Cleanen des Geräts (und anschließender erneuter Push- oder Pull-Bereitstellung) die Datei mit dem GUID nach Abschluss dieses Vorgangs die einzig verbleibende Datei auf dem Gerät ist.

Mit der Option "-f " werden Verzeichnisse gelöscht, deren Eigentümer dieses Produkt ist. Weitere Informationen finden Sie unter Linux-Deinstallationsdokumentation.

Erstellen eines Konfigurationspakets für einen Standalone-Agenten

Normalerweise konfiguriert das Agentenkonfigurationsprogramm SERVERCONFIG.EXE Agenten auf verwalteten Geräten. Sie können jedoch auch im Fenster **Agentenkonfiguration** eine selbstextrahierende ausführbare Datei erstellen lassen, die eine Agentenkonfiguration auf dem Server installiert, auf dem sie ausgeführt wird. Dies ist nützlich, wenn Sie Agenten von einer CD- oder einem mobilem USB-Laufwerk installieren möchten.

Verteilen einer Agentenkonfiguration an Geräte mit einer Push-Prozedur

So stellen Sie eine Agentenkonfiguration mittels Push-Prozedur bereit

1. Wählen Sie in der Konsole die Geräte aus, an die Sie den Agenten verteilen möchten, und klicken Sie dann auf **Ziel**.
2. Klicken Sie im linken Navigationsfenster auf **Agentenkonfiguration**.
3. Klicken Sie mit der rechten Maustaste auf die Agentenkonfiguration, die Sie per Push-Vorgang bereitstellen möchten, und klicken Sie dann auf **Task planen.**
4. Klicken Sie auf **Zielgeräte** im Dialogfeld **Geplante Tasks - Eigenschaften** und klicken Sie dann auf **Zielliste hinzufügen**.
5. Klicken Sie auf **Task planen**.
6. Geben Sie die gewünschte Uhrzeit für die Bereitstellung des Agenten an und klicken Sie auf **Speichern**.

Installieren von Linux-Serveragenten

Sie können Linux-Agenten und RPMs von einem Remote-Standort aus auf Linux-Servern bereitstellen und installieren. Ihr Linux-Server muss für diese Aufgabe richtig konfiguriert sein, da sie sich andernfalls nicht ausführen lässt. Um einen Agenten auf einem Linux-Server installieren zu können, benötigen Sie root-Privilegien.

Die Standardinstallation für Linux (Red Hat 3 und 4 sowie SUSE) beinhaltet die RPMs, die für den Linux-Standard-Verwaltungsagenten erforderlich sind. Wenn Sie den Überwachungsagenten in der **Agentenkonfiguration** auswählen, benötigen Sie ein zusätzliches RPM (sysstat). Eine vollständige Liste der vom Produkt vorausgesetzten RPMs finden Sie im *System Manager Bereitstellungshandbuch*.

Für die erste Linux-Agentenkonfiguration verwendet der Core Server eine SSH-Verbindung, um Linux-Server als Zielserver auswählen zu können. Sie müssen über eine aktive SSH-Verbindung mit Benutzer-/Kennwortauthentifizierung verfügen. Die Produkt unterstützt keine Authentifizierung mittels öffentlichem/privatem Schlüssel. Alle etwaigen Firewalls zwischen dem Core und den Linux-Servern müssen den SSH-Anschluss unterstützen. Testen Sie Ihre SSH-Verbindung auf dem Core Server mit der SSH-Anwendung eines Drittanbieters.

Das Installationspaket für einen Linux-Agenten besteht aus einem Shell-Script, Agenten-Tarball(s), .INI-Agentenkonfiguration und Authentifizierungszertifikaten für den Agenten. Diese Dateien werden in der LDLogon-Freigabe des Core Servers gespeichert. Das Shell-Skript extrahiert Dateien aus dem/den Tarball(s), installiert die RPMs und konfiguriert den Server für das Laden der Agenten und die regelmäßige Ausführung des Inventarscanners in einem von Ihnen in der Agentenkonfiguration festgelegten Intervall. Dateien werden unter /usr/landesk gespeichert.

Sie müssen außerdem den Scheduler-Dienst auf dem Core konfigurieren, um die SSH-Authentifizierungsnachweise (Benutzername/Kennwort) auf Ihrem Linux-Server zu verwenden. Der Scheduler-Dienst verwendet diese Anmeldeinformationen, um die Agenten auf Ihren Servern zu installieren. Verwenden Sie das Programm Dienste konfigurieren, um die SSH-Anmeldeinformationen einzugeben, die der Scheduler-Dienst als alternative

Anmeldeinformationen verwenden soll. Sie werden aufgefordert, den Scheduler-Dienst neu zu starten. Falls diese Aufforderung nicht angezeigt wird, klicken Sie auf **Stopp** und dann auf **Start** auf der Registerkarte **Scheduler**, um den Dienst neu zu starten. Hiermit werden Ihre Änderungen aktiviert.

Bereitstellen von Linux-Agenten

Nachdem Sie die Linux-Server konfiguriert und Linux-Anmeldeinformationen zum Core Server hinzugefügt haben, müssen Sie Server zur Liste **Eigene Geräte** hinzufügen, damit Sie die Linux-Agenten bereitstellen können. Bevor Agenten auf einem Server bereitgestellt werden können, müssen Sie den Server zur Ansicht **Eigene Geräte** hinzufügen. Tun Sie dies, indem Sie Ihre Linux-Server mit der Funktion **Geräteerkennung** erkennen lassen.

So lassen Sie Ihre Linux-Server erkennen

1. Erstellen Sie unter **Geräteerkennung** einen Erkennungstask für jeden Linux-Server. Verwenden Sie einen Standard-Netzwerkscan und geben Sie die IP-Adresse des Linux-Servers als die Start- und Abschluss-IP-Bereiche ein. Wenn Sie mehrere Linux-Server besitzen, geben Sie einen mehrere IP-Adressen umfassenden Bereich ein. Klicken Sie auf **OK**, sobald Sie Ihren Erkennungsbereich hinzugefügt haben.
2. Erstellen Sie einen Zeitplan für den soeben erstellten Erkennungstask, indem Sie auf den Task und dann auf **Planen** klicken. Vergewissern Sie sich nach Abschluss des Vorgangs, dass die zu verwaltenden Linux-Server mithilfe des Erkennungsvorgangs gefunden wurden.
3. Wählen Sie in der **Geräteerkennung** die Server aus, die Sie verwalten möchten, und klicken Sie auf **Ziel**, um die ausgewählten Geräte der Zielliste hinzuzufügen. Klicken Sie in der unteren Fensterhälfte auf die Registerkarte **Verwalten**. Klicken Sie auf **Ausgewählte Geräte verschieben** und klicken Sie dann auf **Verschieben**. Damit werden Server zur Liste **Eigene Geräte** hinzugefügt und stehen als Ziel für Bereitstellungen zur Verfügung.

So erstellen Sie eine Linux-Agentenkonfiguration

1. Klicken Sie in der **Agentenkonfiguration** auf **Neu**.
2. Geben Sie einen Konfigurationsnamen ein, klicken Sie auf **HP-UX**oder **Linux Server Edition**, wählen Sie den Installationstyp aus (Server oder Desktop) und klicken Sie auf **OK**.
3. Wählen Sie die soeben erstellte Konfiguration aus und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die gewünschten Agenten aus.
5. Wählen Sie auf der Registerkarte **Inventar** die Optionen und das gewünschte Scanner-Intervall aus. Das Installationsskript fügt einen Cron-Auftrag hinzu, der den Scanner in dem von Ihnen festgelegten Intervall ausführt.
6. Wählen Sie auf der Registerkarte **Regelsätze** einen Überwachungs- und/oder Alarmregelsatz aus, den Sie in die Konfiguration einfügen möchten. Diese Regelsätze werden im Ordner "ldlogon/alertrules" gespeichert.
7. Klicken Sie auf **Änderungen speichern**.

Um Ihre Agentenkonfiguration bereitzustellen, wählen Sie sie in der **Agentenkonfiguration** aus und klicken Sie auf **Task planen**. Konfigurieren Sie den Task und überwachen Sie den Taskverlauf unter **Konfigurationstasks.**

Hinweis: Sie erhalten erst dann Daten zum Systemzustand auf einem Linux-Gerät, nachdem der Inventarscanner einen ersten Scan nach der Installation ausgeführt hat.

So rufen Sie eine Linux-Agentenkonfiguration mit einer Pull-Prozedur ab

1. Erstellen Sie ein temporäres Verzeichnis auf dem Linux-Gerät (z. B. /tmp/ldcfg) und kopieren Sie Folgendes in dieses temporäre Verzeichnis:
    - Alle Dateien aus dem Verzeichnis "LDLOGON\unix\linux".
    - Das nach der Konfiguration benannte Shell-Skript (<*Konfigurationsname*>.sh).
    - Die nach der Konfiguration benannte *.0-Datei. Das * repräsentiert acht Zeichen (0-9, a-f).
    - Alle in der Datei <*Konfigurationsname*>.ini aufgelisteten Dateien. Um diese Dateien zu identifizieren, durchsuchen Sie die .INI-Datei nach "FILE*xx"*, wobei *xx* einer Zahl entspricht. Die Mehrzahl der Einträge, die Sie finden werden, wurden vom Client in Schritt 1 kopiert; Sie werden jedoch auch .XML-Dateien finden, die kopiert werden müssen. Die Dateinamen sollten, bis auf die folgenden Ausnahmen, nicht geändert werden:
        - alertrules\<*beliebiger Text*>.ruleset.xml sollte in internal.ruleset.xml umbenannt werden.
        - monitorrules\<*beliebiger Text*>.ruleset.monitor.xml sollte in masterconfig.ruleset.monitor.xml umbenannt werden
2. Wenn das Gerät über IPMI und einen BMC verfügt (mit in der Installation eingeschlossener Überwachung), geben Sie Folgendes in einer Befehlszeile ein:

    ```
    export BMCPW="(bmc password)"
    ```

3. Führen Sie das Shell-Skript für die Konfiguration unter Verwendung des folgenden Pfads als Root aus:

    ```
    /tmp/ldcfg/lsminstall.sh
    ```

4. Entfernen Sie das temporäre Verzeichnis einschließlich Inhalt.

Hinweis: Wenn Sie einen Agenten auf einem Linux-Gerät mittels Push- oder Pull-Vorgang bereitstellen, anschließend zum Cleanen des Geräts

```
./linuxuninstall.sh -f ALL
```

ausführen und danach erneut einen Push- oder Pull-Vorgang initiieren, ist die Datei mit dem GUID nach Abschluss dieses Vorgangs die einzig verbleibende Datei auf dem Gerät.

Mit der `-f`-Option werden alle Verzeichnisse gelöscht, die Eigentum des Produkts sind. Weitere Informationen finden Sie unter Linux-Deinstallationsdokumentation.

Befehlszeilenparameter für den Inventarscanner

Der Inventarscanner ldiscan verfügt über verschiedene Befehlszeilenparameter, die festlegen, wie er ausgeführt wird. Eine detaillierte Beschreibung der einzelnen Parameter finden Sie unter "ldiscan -h" oder "man ldiscan". Jeder Option kann entweder '-' oder '/' vorangestellt werden.

Parameter	Beschreibung
-d=Dir	Startet den Softwarescan im Verzeichnis Dir statt im Stammverzeichnis. Standardmäßig beginnt der Softwarescan im Stammverzeichnis.
-f	Erzwingt einen Softwarescan. Wenn Sie -f nicht angeben, führt der Scanner in dem Tagesintervall (standardmäßig täglich) Softwarescans durch, das in der Konsole unter **Konfigurieren | Dienste | Inventar | Scannereinstellungen** angegeben wurde.
-f-	Deaktiviert Softwarescans.
-i=ConfName	Legt den Namen der Konfigurationsdatei fest. Standard ist "/etc/ldappl.conf".
-ntt=address:port	Hostname oder IP-Adresse des Core Servers. Port ist optional.
-o=File	Schreibt Inventarinformationen in die angegebene Ausgabedatei.
-s=Server	Gibt den Core Server an. Dieser Befehl ist optional und ist nur vorhanden, um Abwärtskompatibilität zu gewährleisten.
-stdout	Die Inventarinformationen werden in die Standardausgabe geschrieben.
-v	Aktiviert die Ausgabe ausführlicher Statusmeldungen während der Scan läuft.
-h oder -?	Zeigt den Hilfebildschirm an.

Beispiele

Damit die Daten in eine Textdatei ausgegeben werden, geben Sie Folgendes ein:

```
ldiscan -o=data.out -v
```

Um Daten an den Core Server zu senden, geben Sie Folgendes ein:

```
ldiscan -ntt=ServerIPName -v
```

Linux-Inventarscanner-Dateien

Datei	Beschreibung
ldiscan	Die ausführbare Datei, die mit Befehlszeilenparametern zur Angabe der auszuführenden Aktion aufgerufen wird. Alle Benutzer, die den Scanner ausführen, müssen über ausreichende Berechtigungen zum Ausführen dieser Datei verfügen. Für jede der oben genannten unterstützten Plattformen ist eine eigene Version dieser Datei verfügbar.
/etc/ldiscan.conf	Diese Datei befindet sich immer im Verzeichnis /etc und enthält die folgenden Informationen: • Inventarspezifische eindeutige Kennung • Letzter Hardwarescan • Letzter Softwarescan Alle Benutzer, die den Scanner ausführen, benötigen Lese- und Schreibberechtigungen für diese Datei. Bei der in "in /etc/ldiscan.conf" enthaltenen ID handelt es sich um eine eindeutige Zahl, die dem Computer zugewiesen wird, wenn der Inventarscanner erstmalig ausgeführt wird. Anhand dieser Nummer wird der Computer identifiziert. Falls sich diese Kennung einmal ändert, behandelt der Core Server den Computer als anderen Computer, woraus sich ein doppelter Datenbankeintrag ergibt. **Warnung:** Sie dürfen die eindeutige ID weder ändern noch die Datei "ldiscan.conf" löschen, nachdem sie erstellt wurde.
/etc/ldappl.conf	In dieser Datei passen Sie die Liste der ausführbaren Dateien an, die der Inventarscanner während der Ausführung eines Softwarescans erfasst. Die Datei enthält einige Beispiele, und Sie müssen Einträge für Softwarepakete hinzufügen, die Sie verwenden. Die Suchkriterien basieren auf Dateiname und -größe. Obwohl sich die Datei normalerweise im Verzeichnis /etc befindet, kann der Scanner eine alternative Datei verwenden, die mit dem Befehlzeilenparameter i= angegeben wird.
ldiscan.8	Man-page für ldiscan.

Konsolenintegration

Sobald ein Linux-Computer in die Core-Datenbank gescannt wurde, können Sie Folgendes tun:

- In Abfragen alle Attribute benutzen, die vom Linux-Inventarscanner in die Core-Datenbank ausgegeben werden.
- Mit den Berichtfunktionen Berichte generieren, die vom Linux-Inventarscanner erfasste Informationen enthalten. Beispielsweise wird Linux als BS-Typ im Betriebssystem-Übersichtsbericht angezeigt.
- Inventarinformationen zu Linux-Computern anzeigen.

Abfragen bzgl. der "Systembetriebszeit" werden alphabetisch sortiert und führen zu unerwarteten Ergebnissen
Wenn Sie mithilfe einer Abfrage herausfinden möchten, wie viele Computer länger als eine bestimmte Anzahl von Tagen (beispielsweise 10 Tage) in Betrieb sind, führen Sie eine Abfrage nach dem "Systemstart" anstatt nach der "Systembetriebszeit" durch. Abfragen nach der "Systembetriebszeit" können unvorhersehbare Ergebnisse zurückgeben, da die Systembetriebszeit einfach als eine im Format "x Tage, y Stunden, z Minuten und j Sekunden" formatierte Zeichenfolge verzeichnet wird. Die Sortierung erfolgt daher alphabetisch und nicht nach Zeitintervallen.

Pfad zu den in ldappl.conf referenzierten Dateien wird nicht in der Konsole angezeigt
ConfFile-Einträge in der Datei "ldappl.conf" müssen einen Pfad enthalten.

Geräteüberwachung

Informationen zur Überwachung

System Manager unterstützt mehrere Methoden zur Überwachung des Systemzustands eines Geräts. Überwachungsfunktionen zeichnen Daten aus unterschiedlichen Quellen aus, um Sie bei der Nachverfolgung der vielen unterschiedlichen Daten auf Ihren Geräten zu unterstützen. Die wichtigsten Datenkategorien sind:

- Verwendungsstufen
- Betriebssystemereignisse
- Prozesse und Dienste
- Leistungsprotokolle
- Hardwaresensoren (Lüfter, Spannungswerte, Temperaturen etc.)

Dieses Kapitel enthält Informationen zu den verschiedenen Funktionen, die Ihre verwalteten Geräte überwachen:

- Installieren eines Überwachungsagenten auf Geräten und Erstellen von Überwachungsregelsätzen, die auf Geräten bereitgestellt werden können
- Einrichten von Leistungszählern auf Geräten und Überwachen der Leistungsdaten
- Überwachen von Konfigurationsänderungen mit Alarmierung bei Änderungen
- Regelmäßiges Pingen von Geräten zur Überwachung der Konnektivität mithilfe der Funktion **Geräteüberwachung**

Die Alarmfunktion ist eine verwandte Funktion, die sich des Überwachungsagenten bedient, um Alarmaktionen wie das Senden von E-Mail- oder Pager-Nachrichten, Neustarten oder Herunterfahren eines Geräts oder Hinzufügen von Informationen zum Alarmprotokoll zu initiieren. Alarmaktionen können vom jedem Geräteereignis, das sich überwachen lässt, generiert werden. Weitere Informationen finden Sie unter Verwenden von Alarmen.

Hinweise

- Die Kommunikation mit dem Überwachungsagent erfolgt über HTTP over TCP/IP in Form von GET-, POST- oder XML-Anforderungen. Die Beantwortung von Anforderungen erfolgt in Form von XML- oder HTML-Tabellendokumenten.
- Bevor Sie eine Abfrage zum Zustand eines Geräts (Computer.Health.State) ausführen und speichern, sollten Sie berücksichtigen, dass der Zustand des Servers in der Datenbank durch eine Ziffer repräsentiert wird. Die Ziffern entsprechen folgenden Zuständen: 4=Kritisch, 3=Warnung, 2=Normal, 1=Zu Informationszwecken, Null oder 0=unbekannt.
- Die Hardwareüberwachung ist von der Funktionalität der auf dem Gerät installierten Hardware sowie von der korrekten Konfiguration der Hardware abhängig. Wenn z.B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden keine Überwachungsdaten bereitgestellt.

- Wenn Sie den Eindruck haben, dass die Berichterstellung von einem bestimmten Rechner gestoppt wurde, können Sie mithilfe von "restartmon.exe" im Ordner LDCLIENT den Collector und alle Überwachungsanbieter neu starten. Dieses Dienstprogramm ist für Rechner gedacht, auf denen die Berichterstellung installiert wurde, jedoch keine Berichte mehr erstellt werden. Starten Sie mit diesem Dienstprogramm die Collector und Provider neu, ohne das Gerät neu starten zu müssen.

Bereitstellen des Überwachungsagenten auf Geräten

Wenn der Überwachungsagent auf dem Gerät installiert ist, stellt System Manager eine sofortige Zusammenfassung zum Systemzustand eines Geräts zur Verfügung. Der Überwachungsagent ist einer von sechs Agenten, die auf verwalteten Geräten installiert werden können. Er überprüft die Hardware und Konfiguration eines Geräts in regelmäßigen Abständen und schreibt alle etwaigen Änderungen in den Systemstatus des Geräts. Die Überwachung wird mit dem Zustandssymbol in der Liste **Eigene Geräte** signalisiert; etwaige Details werden in Protokolleinträgen (in der Zusammenfassung **Systeminformationen** für das betreffende Gerät) und in Diagrammen (in der Zusammenfassung **Überwachung** für das betreffende Gerät) angezeigt.

Ein überwachtes Gerät, dessen Festplattenspeicher zunehmend knapper wird, kann das Symbol für eine "Warnung" einblenden, sobald die Festplatte zu 90% ausgelastet ist, und dieses Symbol in das Symbol für den Zustand "Kritisch" ändern, sobald die Auslastung 95% erreicht. Wenn das Gerät über einen Alarmregelsatz für einen Laufwerksspeicheralarm verfügt, erhalten Sie evtl. für denselben Festplattenstatus auch Alarmmeldungen.

Sie können den Standard-Überwachungsregelsatz auf Geräten bereitstellen. Sie haben jedoch auch die Möglichkeit, eigene benutzerdefinierte Regelsätze zu erstellen, die nur die Zustände betreffen, die für Ihr System relevant sind.

Erstellen eines Überwachungsregelsatzes

Sie können entscheiden, was auf einem Gerät überwacht wird, indem Sie einen Überwachungsregelsatz erstellen, der festlegt, was der Überwachungsagent auf dem Gerät überprüft. Sie können einen Regelsatz auf einem einzelnen Gerät oder einer Gruppe mit Zielgeräten bereitstellen. Sie können z.B. einen Regelsatz für Server definieren, die nur Speicheraufgaben wahrnehmen, und einen anderen für Webserver.

Der Standard-Überwachungsregelsatz umfasst 16 Elemente. Beim Erstellen eines Regelsatzes können Sie jedes dieser Elemente ein- oder ausschalten, angeben, wie oft das Element überprüft werden soll, und für bestimmte Elemente Leistungsgrenzwerte festlegen. Sie können zudem auf dem Gerät ausgeführte Dienste überwachen lassen.

Der Prozess für das Erstellen und Bereitstellen eines Regelsatzes sieht wie folgt aus:

1. Wählen Sie die Geräte aus, auf denen Sie den Regelsatz bereitstellen möchten, und klicken Sie dann auf **Ziel**, um sie zur Liste **Zielgeräte** hinzuzufügen.
2. Erstellen oder bearbeiten Sie einen Überwachungsregelsatz. Beachten Sie, dass Sie das Kontrollkästchen aktivieren müssen, um die Überwachung für jedes Ereignis, das überwacht werden soll, im Regelsatz einzuschalten. Nicht für alle Ereignisse ist die Überwachung standardmäßig eingestellt. Einige Ereignisse, z.B. Dienste, setzen voraus, dass Sie jeden zu überwachenden Dienst einzeln auswählen. (Siehe detaillierte Schritte weiter unten.)

3. Stellen Sie den Regelsatz auf den Zielgeräten bereit. Sie können nach Bedarf weitere Geräte als Ziel ansprechen, bevor Sie den Regelsatz bereitstellen. (Siehe detaillierte Schritte weiter unten.)

So erstellen Sie einen Überwachungsregelsatz

1. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
2. Klicken Sie auf **Neu**, geben Sie einen Namen und eine Beschreibung für die Konfiguration ein und klicken Sie auf **OK**.
3. Wählen Sie die Konfiguration in der linken Spalte aus.
4. Klicken Sie in der Liste mit den Elementen auf ein Element, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
5. Um die Überwachung des Elements auszuschalten, deaktivieren Sie das Kontrollkästchen und klicken auf **Aktualisieren**.
6. Um das Intervall für die Überwachung zu ändern, wählen Sie **Sekunden** oder **Minuten** aus und geben eine Zahl in das Textfeld ein.
7. Setzen Sie ggf. die Grenzwerte (in %) für die Zustände "Warnung" und "Kritisch".
8. Wählen Sie zum Überwache von **Diensten** das Betriebssystem aus der Dropdown-Liste aus. Wählen Sie einen oder mehrere zu überwachende Dienste aus (verwenden Sie STRG + Mausklick, um mehrere auszuwählen) und klicken Sie auf **>>**, um die Dienste in die Liste auf der rechten Seite einzufügen.
9. Klicken Sie für jedes von Ihnen geänderte Element auf **Aktualisieren**, um Ihre Änderungen auf die Konfiguration zu übertragen. Wenn Sie ein Element ändern und dann beschließen, die Änderungen nicht zu übernehmen, klicken Sie auf **Zurücksetzen**, um die ursprünglichen Einstellungen wiederherzustellen.

Wenn Sie vom Core Server aus in einer Überwachungskonfiguration enthaltene Dienste bearbeiten, zeigt die Liste **Verfügbare Dienste** bekannte Dienste aus der Inventardatenbank an. Es werden keine Dienste im Listenfeld **Verfügbare Dienste** angezeigt, bis ein LANDesk Agent auf einem oder mehreren Geräten bereitgestellt und ein Inventarscan an den Core zurückgegeben wird. Wenn Sie z. B. einen Linux-Dienst in der Liste auswählen möchten, müssen Sie zunächst einen Agenten auf einem Linux-Gerät bereitstellen.

So stellen Sie einen Überwachungsregelsatz bereit

1. Klicken Sie im linken Navigationsfenster auf **Eigene Geräte** und dann auf die Gruppe **Alle Geräte**.
2. Wählen Sie die Geräte aus, auf denen Sie den Regelsatz bereitstellen möchten, und klicken Sie dann auf **Ziel**, um die Geräte in die Liste **Zielgeräte** aufzunehmen.
3. Klicken Sie im linken Navigationsfenster auf **Überwachung** und klicken Sie dann auf die Registerkarte **Regelsatz bereitstellen**.
4. Wählen Sie auf der Registerkarte **Alarmregelsätze** den Regelsatz aus, den Sie bereitstellen möchten.
5. Klicken Sie auf die Verknüpfung, um die Liste mit den **Zielgeräten** einzublenden. Um ein Gerät aus der Liste zu entfernen, klicken Sie mit der rechten Maustaste auf das Gerät und dann auf **Entfernen**. (Um Geräte hinzuzufügen, müssen Sie sie wie in Stufe 2 beschrieben zur Liste mit den Zielgeräten hinzufügen.)
6. Klicken Sie auf **Bereitstellen**, um den ausgewählten Regelsatz auf den Zielgeräten bereitzustellen.

Als Teil des Bereitstellungsprozesses wird eine XML-Seite erstellt, die den bereitgestellten Regelsatz und die Geräte, auf denen der Regelsatz bereitgestellt wurde, auflistet. Dieser Bericht wird auf dem Core Server im LDLOGON-Verzeichnis gespeichert und mit einer fortlaufenden Nummer benannt, die ihm von der Datenbank zugewiesen wird. Wenn Sie diese XML-Seite unabhängig vom Bereitstellen eines Regelsatzes anzeigen möchten, klicken Sie auf die Schaltfläche **XML generieren** und klicken dann auf die Verknüpfung, mit der die XML-Datei angezeigt wird. Die Generierung eines Regelsatzes als XML-Datei hat zudem den Vorteil, dass der Regelsatz in der Liste der verfügbaren Regelsätze in den **Einstellungen für die Agentenkonfiguration** dargestellt werden kann.

Deaktivieren des ModemView-Dienstes

Der ModemView-Dienst ist der Dienst/Treiber, der Modemanrufe (sowohl ankommende als auch ausgehende) überwacht und einen Alarm generiert, wenn ein Anruf registriert wird. Dieser Dienst beansprucht 10 MB, da er mit MFC arbeitet. Es ist für Sie u.U. nicht sinnvoll, diesen Dienst auszuführen, insbesondere, wenn kein Modem an das Gerät angeschlossen ist.

So deaktivieren Sie den ModemView-Dienst

1. Klicken Sie auf dem Gerät (entweder direkt oder remote) auf **Start** > **Systemsteuerung** > **Verwaltung** > **Dienste**.
2. Doppelklicken Sie auf **LANDesk Message Handler Service**.
3. Wählen Sie unter **Starttyp** die Einstellung **Manuell** aus und klicken Sie auf **OK**.

Sie können auch auf **Beenden** unter **Dienststatus** klicken.

Einstellen von Leistungszählern

System Manager gibt Ihnen die Möglichkeit, Leistungselemente (Zähler) auszuwählen, die Sie auf einem verwalteten Gerät überwachen möchten. Sie können zahlreiche unterschiedliche Elemente überwachen, einschließlich Hardwarekomponenten (beispielsweise Laufwerke, Prozessoren und Speicher), Betriebssystemkomponenten (beispielsweise Prozesse) oder Anwendungskomponenten (vom Webserver des Systems übertragene Byte/Sek o. ä.). Beim Auswählen eines Leistungszählers geben Sie auch das Abfrageintervall für das betreffende Element an, definieren Grenzwerte für die Leistung und legen fest, wie oft die Grenzwerte überschritten werden dürfen, ehe ein Alarm generiert wird.

Nachdem Sie einen Leistungszähler ausgewählt haben, können Sie die Leistung auf der Seite **Überwachung** nachverfolgen, indem Sie ein aus Echtzeit- oder Vergangenheitsdaten generiertes Diagramm anzeigen. Weitere Informationen finden Sie unter Leistungsüberwachung.

So wählen Sie einen zu überwachenden Leistungszähler aus

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem anderen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
3. Klicken Sie auf die Registerkarte **Einstellungen für die Leistungszähler**.
4. Wählen Sie in der Spalte **Objekte** das zu überwachende Objekt aus.
5. Wählen Sie in der Spalte **Instanzen** ggf. die Instanz des zu überwachenden Objekts aus.

6. Wählen Sie in der Spalte **Zähler** den zu überwachenden Zähler aus.

   Wenn der gewünschte Zähler nicht in der Liste angezeigt wird, klicken Sie auf **Zähler neu laden**, um die Liste mit neuen Objekten, Instanzen oder Zählern zu aktualisieren.

7. Geben Sie das Abfrageintervall an (**Überprüfen alle** *n* **Sekunden**) und die Anzahl von Tagen, die der Zählerverlauf gespeichert werden soll.
8. Geben Sie im Textfeld **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** an, wie oft der Zähler die Grenzwerte überschreiten darf, ehe ein Alarm generiert wird.
9. Geben Sie die unteren und/oder oberen Grenzwerte an.
10. Klicken Sie auf **Übernehmen**.

Hinweise

- Protokolldateien können rasch an Volumen zunehmen. Allein durch das Abfragen eines einzelnen Zählers im Zwei-Sekunden-Intervall wächst das Leistungsprotokoll täglich um 2,5 MB.
- Eine Warnmeldung wird generiert, wenn ein Leistungszähler auf einem Windows- oder einem Linux-Gerät unter einen Grenzwert fällt. Wenn ein Leistungszähler auf einem Linux-Gerät einen oberen Grenzwert überschreitet, wird eine Warnmeldung generiert. Wenn ein Leistungszähler auf einem Windows-Gerät einen oberen Grenzwert überschreitet, wird eine kritische Warnung generiert.
- Berücksichtigen Sie beim Einrichten von Grenzwerten, dass Alarme generiert werden, ganz gleich, ob ein oberer oder unterer Grenzwert überschritten wird. Bei einem Grenzwert, der sich auf die verfügbare Speicherplatzmenge bezieht, möchten Sie wahrscheinlich nur benachrichtigt werden, wenn der Speicherplatz knapp wird. In diesem Fall, sollten Sie den oberen Grenzwert so hoch setzen, dass Sie nicht benachrichtigt werden, wenn auf dem Gerät eine große Menge Speicherplatz verfügbar wird.
- Indem Sie den Wert für **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** ändern, können Sie die Aufmerksamkeit auf ein hartnäckiges Problem oder ein isoliertes Ereignis lenken. Wenn Sie beispielsweise die von einem Webserver gesendeten Byte überwachen, kann System ManagerSie alarmieren, wenn der Byte/Sek.-Wert konstant überhöht ist. Oder Sie können einen niedrigen Wert wie 1 oder 2 angeben, um eine Alarmnachricht zu erhalten, sobald Ihre anonymen FTP-Verbindungen eine bestimmte Anzahl von Benutzern überschreiten.

Leistungsüberwachung

Auf der Seite **Überwachung** können Sie die Leistung unterschiedlicher Systemobjekte überwachen. Sie können spezifische Hardwarekomponenten (Laufwerke, Prozessoren und Speicher) oder Betriebssystemkomponenten (Prozesse oder vom Webserver des Systems übertragene Byte/Sek.) überwachen. Die Seite **Überwachung** enthält ein Diagramm, das Echtzeitdaten oder Vergangenheitsdaten für Zähler anzeigt.

Um einen Leistungszähler zu überwachen, müssen Sie den Zähler zunächst auswählen. Hierbei wird der Zähler in die Liste der überwachten Zähler eingefügt. Bei diesem Vorgang geben Sie auch die Polling-Häufigkeit für das betreffende Element an, definieren Grenzwerte für die Leistung und legen fest, wie oft die Grenzwerte überschritten werden dürfen, bevor ein Alarm

generiert wird. Weitere Informationen zum Auswählen von Leistungszählern finden Sie im Thema Einrichten von Leistungszählern.

So zeigen Sie das Leistungsdiagramm für einen überwachten Zähler an

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem anderen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
3. Klicken Sie nach Bedarf auf die Registerkarte **Aktive Leistungszähler**.
4. Wählen Sie in der Dropdown-Liste **Zähler** den Zähler aus, für den Sie ein Leistungsdiagramm anzeigen möchten.
5. Wählen Sie **Echtzeitdaten anzeigen**, um ein Diagramm der Echtzeitleistung einzublenden.

   Oder

   wählen Sie **Protokolldaten anzeigen**, um ein Diagramm einzublenden, das über die Leistung Auskunft gibt, die während des Zeitraums erzielt wurde, den Sie beim Auswählen des Zählers (mit der Option "Verlauf speichern") festgelegt hatten.

Im Leistungsdiagramm repräsentiert die Horizontalachse den verstrichenen Zeitraum. Die Vertikalachse repräsentiert die gemessenen Einheiten, beispielsweise Byte/Sek. (beim Überwachen von Dateiübertragungen), Prozent (beim Überwachen des Prozentsatzes der CPU-Nutzung) oder verfügbare Byte (beim Überwachen des Festplattenspeichers). Die Linienhöhe ist eine flexible Einheit. Sie ändert sich je nach Datenextrem; für den einen Zähler kann die Vertikalachse z.B. 1 bis 100 repräsentieren und für einen anderen vielleicht 1 bis 500.000. Bei Daten mit extremer Variationsbreite können minimale Änderungen als flache Linie erscheinen.

Hinweise

- Beim Auswählen eines anderen Zählers wird das Diagramm aktualisiert und die Maßeinheit zurückgesetzt.
- Klicken Sie auf **Aktualisieren**, um den Inhalt des Diagramms zu löschen und neu zu starten.
- Wenn Sie einen Alarm erhalten, der von einem in der Liste geführten Zähler generiert wurde, klicken Sie mit der rechten Maustaste auf den Zähler und klicken auf **Bestätigen**, um den Alarm zurückzusetzen.

So beenden Sie die Überwachung eines Leistungszählers

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem anderen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
3. Klicken Sie nach Bedarf auf die Registerkarte **Aktive Leistungszähler**.
4. Klicken Sie unter **Überwachte Leistungszähler** mit der rechten Maustaste auf den Zähler und klicken Sie auf **Löschen**.

Überwachen von Konfigurationsänderungen

Dieses Produkt kann einen Alarm generieren, wenn sich die Hardware- oder Softwarekonfiguration eines Geräts ändert und der Überwachungsagent auf dem Gerät installiert ist. Änderungen in der Hardware- und Softwarekonfiguration können sich auf die Leistung und Stabilität eines Geräts auswirken oder Probleme für eine Standardinstallation verursachen. Indem Sie wichtige Komponenten eines Geräts überwachen lassen, können Sie mit diesem Produkt die Gesamtbesitzkosten (TCO, Total Cost of Ownership) reduzieren.

Zu den Änderungen in der Gerätekonfiguration, die einen Alarm auslösen, gehören:

- **Anwendung installiert oder deinstalliert:** Sie können sehen, welche Benutzer Anwendungen installiert oder entfernt haben. Diese Informationen können sich für die Überwachung der Lizenznutzung oder Mitarbeiterproduktivität als nützlich erweisen. Es werden die Anwendungen überwacht, die im Windows-Bereich "Software" in der Systemsteuerung registriert sind. Andere Anwendungen werden ignoriert. Der Programmname, der in Windows unter "Software" verwendet wird, entspricht dem im Benachrichtigungsprotokoll oder Popup-Alarmfenster angezeigten Programmnamen.
- **Speicher wurde hinzugefügt oder entfernt:** Dieses Produkt erkennt und überwacht die Speichermenge und den Speichertyp, die/der installiert wurde. Ändert sich die Konfiguration, so wird ein Alarm generiert.
- **Festplatten hinzugefügt oder entfernt:** Dieses Produkt erkennt und überwacht den auf den Geräten installierten Festplattentyp und die Festplattengröße. Ändert sich die Konfiguration, so wird ein Alarm generiert.
- **Prozessor (oder Prozessoren) hinzugefügt, entfernt oder geändert:** Dieses Produkt erkennt und überwacht Prozessoranzahl, -typ und -geschwindigkeit. Ändert sich die Konfiguration, so wird ein Alarm generiert.
- **Netzwerkkarte hinzugefügt oder entfernt:** Dieses Produkt erkennt und überwacht die Anzahl von Netzwerkkarten und Netzwerkkartentypen auf Geräten und generiert einen Alarm, wenn sich die Konfiguration ändert.

Um einen Datensatz mit Alarmmeldungen anzuzeigen, die aus Konfigurationsänderungen resultieren, überprüfen Sie das Alarmprotokoll in der Serverinformationskonsole. Weitere Informationen finden Sie unter Anzeigen des Alarmprotokolls.

Überwachen der Konnektivität

In den meisten Fällen können Geräte Sie beim Eintreten kritischer Situationen alarmieren, z. B., wenn die Speicherressourcen auf der Festplatte knapp werden oder der Lüfter nicht mehr arbeitet. In bestimmten Situationen kann es jedoch passieren, dass das Gerät offline geht, bevor es einen Alarm senden kann. Beispiel: Ein Schalter oder Router unterbricht den Netzwerkverkehr oder die Stromzufuhr des Geräts fällt aus.

In diesen Situationen kann das vorliegende Produkt Geräte in regelmäßigen Abständen daraufhin prüfen, ob sie noch im Netzwerk zur Verfügung stehen. Wenn das Gerät auf den Ping-Test nicht reagiert, wird sein Zustand im Dashboard in "kritisch" geändert das nächste Mal, wenn Sie die Liste **Eigene Geräte** aktualisieren.

Sie müssen die Geräteüberwachung für das Pingen von Zielgeräten oder allen Geräten in der Gruppe **Alle Geräte** einrichten.

So richten Sie die Geräteüberwachung ein

1. Wählen Sie in der Liste **Eigene Geräte** die Geräte aus, die Sie überwachen möchten. Sie können sie aus der Liste **Alle Geräte** oder aus einer öffentlichen oder privaten Gruppe auswählen.
2. Klicken Sie auf **Ziel**.
3. Klicken Sie im unteren Fensterausschnitt auf **Aktionen** und klicken Sie dann auf **Geräteüberwachung**.
4. Zum Anzeigen einer Liste mit gegenwärtig überwachten Geräten klicken Sie auf **Überwachte Geräte anzeigen**.
5. Geben Sie das Minutenintervall zwischen den Ping-Durchläufen an und legen Sie fest, wie oft das Produkt versuchen wird, mit einem Gerät zu kommunizieren.
6. Wählen Sie aus, ob die Aktion auf Geräten in der Liste "Zielgeräte" oder auf allen Geräten in der Gruppe **Alle Geräte** ausgeführt werden soll.
7. Wählen Sie **Nie einen Ping-Test mit dem Gerät durchführen** aus, um die Überwachung einzustellen.
8. Klicken Sie auf **Übernehmen**.

Nur die letzte Gruppe mit Zielgeräten wird überwacht. Wenn Sie z. B. Gerät A und Gerät B als Ziel auswählen und die Geräteüberwachung auf diese Geräte anwenden, werden nur Gerät A und Gerät B vom Core Server einem Ping-Test unterzogen. Wenn Sie anschließend Gerät C und Gerät D als Zielgeräte auswählen und die Geräteüberwachung auf diese Geräte anwenden, werden nur Gerät C und Gerät D überwacht, nicht mehr A und B.

Alarmkonfiguration

Verwenden von Alarmen

Wenn auf einem Gerät Probleme auftreten oder andere Ereignisse registriert werden (z. B. eine Verknappung der Speicherressourcen), kann System Manager eine Alarmmeldung zustellen. Sie können diese Alarme an Ihre Anforderungen anpassen, indem Sie den Schweregrad oder Grenzwert, der den Alarm auslösen wird, auswählen. Alarme werden an die Konsole weitergeleitet und lassen sich für die Durchführung bestimmter Aktionen konfigurieren. Informieren Sie sich in diesem Kapitel über die Funktionsweise der Alarme.

- Wie erhalte ich Alarmnachrichten?
- Welche Geräteprobleme können einen Alarm auslösen?
- Konfigurieren des Schweregrads für Ereignisse
- Prozess für das Konfigurieren von benutzerdefinierten Alarmregelsätzen
- Beispiel: Konfigurieren eines Regelsatz für die Alarmierung bei Verknappung von Festspeicherressourcen

Wie erhalte ich Alarmnachrichten?

Dieses Produkt kann Sie wie folgt über Probleme oder andere Computerereignisse informieren:

- Hinzufügen von Informationen zum Protokoll
- Benachrichtigung per E-Mail oder Übermittlung einer Pager-Nachricht
- Ausführen eines Programms auf dem Core oder auf einem bestimmten Gerät
- Weiterleiten einer SNMP-Trap an eine SNMP-Verwaltungskonsole im Netzwerk
- Neustarten oder Herunterfahren eines Geräts

Beachten Sie, dass bestimmte Alarme, die Rechnergruppen zugeordnet wurden, gleichzeitig eine große Anzahl von Antworten generieren können. Beispiel: Sie konfigurieren den Alarm "Computerkonfiguration wurde geändert" und verknüpfen ihn mit einer E-Mail-Aktion. Wenn ein Softwareverteilungs-Patch auf die Rechner übertragen wird, auf denen diese Alarmeinstellung aktiviert wurde, würde durch dieses Patch auf dem Core Server eine ebenso große Anzahl von E-Mails generiert wie Rechner, auf die das Patch übertragen wurde; d.h., auf Ihre E-Mail-Server käme möglicherweise eine Flut von E-Mails zu. In diesem Fall besteht die Lösung möglicherweise darin, den Alarm ganz einfach in das Core-Protokoll zu schreiben, anstatt E-Mails zu senden.

Welche Geräteprobleme können einen Alarm auslösen?

Dieses Produkt verfügt über eine umfassende Liste mit Ereignissen, die Alarme auslösen können. Einige Probleme bedürfen Ihrer sofortigen Aufmerksamkeit, andere sind Konfigurationsänderungen, die möglicherweise ein Problem darstellen können, die einem Systemadministrator jedoch wertvolle Informationen zur Verfügung stellen. (Weitere Informationen im Zusammenhang mit diesem Thema finden Sie unter Überwachen von Konfigurationsänderungen.) Alarme können nur generiert werden, wenn Geräte mit der entsprechenden Hardware ausgerüstet sind. Von einem Sensor generierte Alarme sind nur für Geräte relevant, die mit den korrekten Sensoren ausgestattet sind.

Zu den Ereignissen, die potenziell überwacht werden können, gehören u.a.:

- **Hardwareänderung:** Eine Komponente, beispielsweise ein Prozessor, ein Speichermodul, ein Laufwerk oder eine Karte, wurden hinzugefügt oder entfernt.
- **Hinzugefügte oder entfernte Anwendung:** Eine Anwendung wurde auf einem Gerät installiert oder deinstalliert.
- **Dienstereignis:** Auf dem Gerät wurde ein Dienst gestartet oder gestoppt.
- **Leistung:** Ein Leistungsgrenzwert wurde überschritten, beispielsweise die Laufwerkskapazität, verfügbarer Speicherplatz etc.
- **IPMI-Ereignis:** Ein Ereignis, das auf IPMI-Geräten registriert werden kann, ist aufgetreten - beispielsweise Änderungen an den Controllern, Sensoren, Protokollen etc.
- **Modemverwendung:** Das Systemmodem wurde benutzt, oder ein Modem wurde hinzugefügt oder entfernt.
- **Physikalische Sicherheit:** Erkennung einer Gehäusemanipulation (Intrusion Detection), Power Cycling oder eine andere physikalische Änderung.
- **Paketinstallation**: Auf dem Zielcomputer wurde ein Paket installiert.
- **Fernsteuerungsaktivität:** Aktivität im Zusammenhang mit einer Fernsteuerungssitzung wurde registriert, einschließlich Start, Stopp oder Fehler.

Hardwareüberwachungsfunktionen, die Alarme generieren, sind von der Funktionalität der auf dem Gerät installierten Hardware sowie von der korrekten Konfiguration der Hardware abhängig. Wenn z.B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden durch die S.M.A.R.T.-Laufwerksüberwachung keine Alarme generiert.

Konfigurieren des Schweregrads für Ereignisse

Geräteprobleme oder Ereignisse können mit einigen oder allen der nachstehend genannten Schweregrade verknüpft werden.

- **Zu Informationszwecken:** Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen. Dieser Schweregrad wirkt sich nicht auf den Gerätezustand aus.
- **OK:** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.
- **Warnung:**Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
- **Kritisch:** Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Unbekannt:** Der Alarmstatus lässt sich nicht bestimmen oder der Überwachungsagent ist nicht auf dem Gerät installiert.

Je nachdem, um welches Ereignis oder Serverproblem es sich handelt, sind einige Schweregrade nicht relevant und bleiben deshalb unberücksichtigt. Beispiel: Bei einem Intrusion Detection-Ereignis ist das Gehäuse des Geräts entweder offen oder geschlossen. Wenn es offen ist, kann dies eine Warnaktion mit dem Schweregrad "Warnung" auslösen. Andere Ereignisse, z. B. "Festplattenspeicher" und "Virtueller Speicher", umfassen drei Warnstufen ("OK", "Warnung" und "Kritisch").

Sie können den Schweregrad oder Grenzwert auswählen, der bestimmte Alarme auslösen wird. Sie können beispielsweise unterschiedliche Alarmaktionen als Reaktion auf den Status

"Warnung" oder "Kritisch" auswählen. Der Status "Unbekannt" kann nicht als Alarmauslöser ausgewählt werden; er gibt lediglich an, dass sich der Status nicht bestimmen lässt.

Prozess für das Konfigurieren von benutzerdefinierten Alarmregelsätzen

Sie können einen Satz Alarmregeln konfigurieren und auf einem bestimmten Gerät oder einer Gruppe mit Zielgeräten bereitstellen. Auf jedem verwalteten Gerät muss die Überwachungskomponente des Produkts installiert sein, damit es den Core Server alarmieren kann. (Weitere Informationen finden Sie unter Konfigurieren von Agenten.)

Beim Installieren der Überwachungskomponente auf einem verwalteten Gerät wird auch ein Standardsatz Alarmregeln installiert, um Feedback-Meldungen bzgl. des Systemzustands an das Konsole weiterzuleiten. Dieser Satz Standardregeln schließt u.a. folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Leistungsüberwachung
- IPMI-Ereignisse (auf relevanter Hardware)

Zusätzlich zu diesem Standardregelsatz können Sie benutzerdefinierte Alarmregelsätze konfigurieren und bereitstellen. Sie können in diese Gruppen benutzerdefinierte Alarmaktionen einschließen, um auf ein bestimmtes Ereignis zu reagieren. Beispiel: Wenn ein Lüfter den Betrieb einstellt, kann er einen Alarm auslösen und eine E-Mail an Ihre Hardware-Supportgruppe senden.

Der Prozess für das Erstellen und Bereitstellen eines Regelsatzes sieht wie folgt aus:

1. Wählen Sie die Geräte aus, auf denen Sie den Regelsatz bereitstellen möchten, und klicken Sie dann auf **Ziel**, um sie zur Liste **Zielgeräte** hinzuzufügen.
2. Erstellen Sie die Alarmaktions-Regelsätze, die Sie verwenden möchten. Diese Aktionsregelsätze definieren die Aktionstypen, die von Alarmen ausgelöst werden können. (Weitere Informationen erhalten Sie unter Konfigurieren von Alarmaktionen.)
3. Erstellen Sie einen benutzerdefinierten Alarmregelsatz.. Hierbei können Sie die Aktionen auswählen, die Sie zuvor definiert haben. (Weitere Informationen finden Sie unter Konfigurieren eines Alarmregelsatzes).
4. Stellen Sie den Regelsatz auf den Zielgeräten bereit. Sie können weitere Geräte als Ziel ansprechen, bevor Sie den Regelsatz bereitstellen. (Weitere Informationen finden Sie unter Bereitstellen von Regelsätzen).

Das folgende Beispiel veranschaulicht, einen einfachen Konfigurationsprozess für einen Regelsatz.

Beispiel: Konfigurieren eines Regelsatz für die Alarmierung bei Verknappung von Festspeicherressourcen

1. Klicken Sie im linken Navigationsfenster auf **Eigene Geräte** und dann auf die Registerkarte **Alle Geräte**.

2. Wählen Sie die Geräte aus, für die Sie einen Alarm einstellen möchten, klicken Sie auf **Ziel**, um die Geräte in der Liste **Zielgeräte** zu platzieren.
3. Klicken Sie auf **Alarmierung** und klicken Sie dann auf die Registerkarte **Aktion-Regelsätze**.
4. Wählen Sie in der Dropdown-Liste **Aktionen** die Aktion aus, die Sie konfigurieren möchten (z. B. **Senden einer E-Mail/Pager-Nachricht**). Klicken Sie auf **Neu**, geben Sie einen Namen in das Feld **Name** ein und klicken Sie auf **OK**.
5. Sobald wieder die Seite **Aktion-Regelsätze** angezeigt wird, wählen Sie den Regelsatz aus, dem Sie soeben einen Namen zugewiesen haben, und klicken dann auf **Aktionen bearbeiten**. Geben Sie die Daten wie angefordert in die Textfelder ein. Klicken Sie abschließend auf **Speichern**.
6. Klicken Sie auf die Registerkarte **Alarm-Regelsätze**.
7. Klicken Sie auf **Neu**, geben Sie einen Hinweis wie "Problem mit dem Festplattenspeicher" in das Feld **Name** ein, geben Sie eine Beschreibung in das Feld **Beschreibung** ein und klicken Sie auf **OK**.
8. Klicken Sie auf den von Ihnen soeben benannten Alarm-Regelsatz und klicken Sie auf **Regelsatz bearbeiten**.
9. Klicken Sie auf die Schaltfläche **Neu**.
10. Klicken Sie in der Dropdown-Liste **Alarmtyp** auf **Laufwerkspeicherplatz**.
11. Aktivieren Sie den Status, für den ein Alarm ausgelöst werden soll: **OK**, **Warnung** oder **Kritisch**. (Wenn Sie dieselbe Aktion für mehrere Zustände initiieren möchten, wählen Sie mehrere aus). Wenn Sie für jeden Status eine andere Aktion initiieren möchten, erstellen Sie eine separate Konfiguration für jeden Status, damit Sie unterschiedliche Aktionen für unterschiedliche Statusstufen auslösen können.)
12. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, die ausgeführt werden soll, wenn die in Schritt 6 und 7 angegebenen Bedingungen eintreten. Wenn die gewünschte Aktion nicht in der Liste angezeigt wird, können Sie sie erstellen. Öffnen Sie dazu die Seite **Aktion-Regelsätze**. (Wenn Sie keinen Regelsatz für eine Alarmaktion konfiguriert haben, wird dieser auch nicht in der Liste angezeigt.)
13. Wählen Sie hierfür in der Dropdown-Liste **Alarmaktion** die gewünschte Konfiguration aus.
14. Aktivieren Sie das Kontrollkästchen **Hat Auswirkungen auf den Gerätezustand**, wenn Sie veranlassen möchten, dass der Alarm auf den Zustand des Servers angewendet wird, wenn dieser im in der Liste **Alle Geräte** angezeigt wird. Wenn der Schweregrad für den Alarm **Zu Informationszwecken** entspricht, wirkt sich der Alarm nicht auf den Gerätezustand aus.
15. Klicken Sie auf **Hinzufügen**.
16. Wiederholen Sie die Schritte 6-12, um zusätzliche Alarme zum Regelsatz hinzuzufügen.
17. Klicken Sie nach Eingabe aller erforderlichen Daten auf **Schließen**.
18. Wenn Sie einen Alarmtyp im Regelsatz ändern möchten, wählen Sie den Alarmtyp aus und klicken Sie auf **Bearbeiten**, nehmen Sie die Änderungen vor, klicken Sie auf **Aktualisieren** und klicken Sie dann auf **Schließen**.
19. Wenden Sie anschließend den definierten Alarmregelsatz auf die Zielgeräte an: Klicken Sie auf **Regelsatz bereitstellen**, wählen Sie den Regelsatz aus und klicken Sie auf **Bereitstellen**.

Konfigurieren von Alarmaktionen

Verwenden Sie die Seite **Aktion-Regelsätze**, um zusätzliche Informationen dazu bereitzustellen, wie sich Aktionen verhalten sollen, wenn sie ausgewählt werden. Bei der Überschreitung eines Grenzwertes wird ein Alarm ausgelöst. Mit dem Alarm kann eine Aktion verknüpft sein,

beispielsweise das Senden einer E-Mail-Nachricht. Jede Aktion besitzt ihre eigenen Konfigurationen und muss individuell konfiguriert werden.

So erstellen Sie einen Aktionsregelsatz

1. Klicken Sie im linken Navigationsfenster auf **Alarmierung** und klicken Sie dann auf die Registerkarte **Aktion-Regelsätze**.
2. Wählen Sie in der Dropdown-Liste **Aktionen** die Aktion aus, die Sie konfigurieren möchte. Jede Aktion verfügt über eine eigene Liste eindeutiger Konfigurationen.
3. Klicken Sie auf **Neu**, geben Sie einen Namen in das Feld **Name** ein und klicken Sie auf **OK**.
4. Sobald wieder die Seite **Aktion-Regelsätze** angezeigt wird, wählen Sie den Regelsatz aus, dem Sie soeben einen Namen zugewiesen haben, und klicken dann auf **Aktionen bearbeiten**.
5. Wenn Sie **Anwendung auf dem Core ausführen** oder **Anwendung auf dem Client ausführen** ausgewählt haben, geben Sie den Pfad zu dem Programm ein, das beim Auslösen des Alarms ausgeführt werden soll, und klicken Sie dann auf **Speichern**. Beachten Sie beim Auswählen einer der beiden Aktionen vom Typ **Programm ausführen**, dass Programme möglicherweise nicht wie erwartet auf dem Desktop angezeigt werden. Wenn die Anwendung ausgeführt wird, wird sie als Dienst in Windows gestartet und deshalb nicht so angezeigt wie eine reguläre Anwendung. Anwendungen, die auf diese Weise ausgeführt werden, sollten keine Benutzeroberfläche enthalten, die Eingaben erfordert. Um mit letzter Sicherheit festzustellen, ob das Programm ausgeführt wurde, überprüfen Sie die Prozesse im Windows Task Manager.

   Wenn Sie **E-Mail/Page senden** ausgewählt haben, geben Sie die vollständige E-Mail-Adresse der Person, die die E-Mail erhalten soll, in das Feld **An** ein; geben Sie eine gültige E-Mail-Adresse in das Feld **Von** ein, geben Sie einen Betreff in das Feld **Betreff** ein, geben Sie eine Nachricht in das Feld **Hauptteil** ein, wählen Sie den Tag oder die Uhrzeit aus, an dem bzw. zu der die Nachricht gesendet werden soll. Geben Sie abschließend den Speicherort eines SMTP-Servers in das Feld **SMTP-Server** ein. Klicken Sie auf das Feld **Hilfe**, um zu erfahren, wie Sie Nachrichten an mehrere Empfänger gleichzeitig senden und Variablen in Ihren Nachrichtentexten verwenden können. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

   Wenn Sie **SNMP-Trap senden** ausgewählt haben, geben Sie den Host-Namen ein, wählen eine Version aus, geben den Community-String in das Feld **Community-String** ein und klicken auf **Speichern**.

Hinweise

- Bestimmte Alarme, die Computergruppen zugeordnet wurden, können simultan eine große Anzahl von Antworten generieren. Beispiel: Sie konfigurieren den Alarm "Computerkonfiguration wurde geändert" und verknüpfen ihn mit einer E-Mail-Aktion. Wenn ein Softwareverteilungs-Patch auf die Rechner übertragen wird, auf denen diese Alarmeinstellung aktiviert wurde, würde durch dieses Patch auf dem Core Server eine ebenso große Anzahl von E-Mails generiert wie Rechner, auf die das Patch übertragen wurde; d.h., auf Ihre E-Mail-Server käme möglicherweise eine Flut von E-Mails zu. In diesem Fall besteht die Lösung möglicherweise darin, den Alarm ganz einfach in das Core-Protokoll zu schreiben, anstatt E-Mails zu senden.

- Einige Alarmaktionen wirken sich nicht auf den Gerätezustand aus. Zu diesen Aktionen gehören u. a. "Programm auf dem Client ausführen", "Herunterfahren/Neu starten" und jeder Alarm mit rein informativem Charakter. Wird eine von diesen Aktionen jedoch mit anderen Alarmaktionen kombiniert wird, die sich auf den Gerätezustand auswirken, so bedeutet dies, dass jeder generierte Alarm sich auf den Gerätezustand auswirkt und in das Alarmprotokoll geschrieben wird.
- Das Feld **Von** in der E-Mail-Nachricht muss eine gültige E-Mail-Adresse enthalten, da die SMTP-Alarmierung andernfalls nicht funktionsfähig ist.
- Als Version 1 identifizierte SNMP-Traps werden verarbeitet, während die als Version 3 identifizierten Traps nur weitergeleitet werden.
- Für SNMP-Traps werden die Schweregradstufen im Feld "Specific Trap Type" der Trap registriert. Gülte Werte sind: 1 = unbekannt, 2 = Info, 3 = OK, 4 = Warnung, 5 = kritisch

Konfigurieren eines Alarmregelsatzes

Verwenden Sie die Seite **Alarmregelsätze**, um einen neuen Alarmregelsatz zu erstellen. Vor dem Konfigurieren eines Alarms müssen Sie Aktionen konfigurieren. (Weitere Informationen erhalten Sie unter Konfigurieren von Alarmaktionen.)

Es gibt zwei Alarmregelsätze, die standardmäßig auf der Seite **Alarmregelsätze** angezeigt werden:

- **Core-Alarmregelsatz**: Dieser Regelsatz gewährleistet, dass Alarme an den Core Server gesendet werden, wenn die Funktion **Geräteüberwachung** aktiviert ist (siehe Überwachung auf Konnektivität). Dieser Regelsatz enthält eine vordefinierte Gruppe mit Alarmen, einschließlich Alarme des Typs "Gerätemonitor", "AMT Circuit Breaker" und "Serial Over LAN Session". Sie können den Status, die Aktion, die Alarmaktion und Health-Einstellungen für die Core-Alarmtypen ändern; alle anderen versuchten Änderungen werden jedoch ignoriert.
- **Standardregelsatz**: Dieser Regelsatz wird auf allen verwalteten Geräten bereitgestellt und enthält eine Reihe von Alarmtypen, die den meisten Netzwerkadministratoren zur allgemeinen Verwendung dienen. Sie können diesen Regelsatz bearbeiten, um andere Alarmtypen hinzuzufügen und die Einstellungen für die Standard-Alarmtypen zu ändern. Wenn Sie diesen Regelsatz bearbeiten, werden die Änderungen auf allen verwalteten Geräten bereitgestellt, selbst wenn Sie den Regelsatz nicht explizit neu bereitstellen.

Zusätzlich zu diesen Regelsätzen können Sie benutzerdefinierte Regelsätze erstellen, um sie auf Zielgruppen mit verwalteten Geräten anzuwenden. Diese Regelsätze müssen im XML-Format generiert werden, damit sie in der **Agentenkonfiguration** angezeigt werden.

Berücksichtigen Sie beim Erstellen eines benutzerdefinierten Regelsatzes für ein bestimmtes Gerät, dass sich überschneidende oder miteinander in Konflikt stehende Alarmregeln vorhanden sein können (falls bereits ein Standardregelsatz auf dem Gerät bereitgestellt wurde). Wenn Sie den Standardregelsatz beim Konfigurieren des verwalteten Geräts bereitstellen und dann einen benutzerdefinierten Regelsatz bereitstellen, werden beide Regelsätze auf dem Gerät ausgeführt. Beispiel: Wenn beide Regelsätze Alarme für denselben Alarmtyp generieren, jedoch unterschiedliche Aktionen in die Wege leiten, müssen Sie damit rechnen, dass Alarmaktionen doppelt ausgeführt werden oder unvorhersehbare Folgen haben. Haben Sie den Standardregelsatz erst einmal bereitgestellt, können Sie ihn zwar nicht mehr entfernen, jedoch können Sie ihn beliebig bearbeiten.

So erstellen Sie einen Alarmregelsatz

1. Klicken Sie im linken Navigationsfenster auf **Alarmierung** und dann auf die Registerkarte **Alarmregelsätze** (falls erforderlich).
2. Klicken Sie auf **Neu**, geben Sie einen Namen in das Feld **Name** ein, geben Sie eine Beschreibung des Alarms in das Feld
   Beschreibung ein und klicken Sie dann auf **OK**.
3. Klicken Sie auf den soeben benannten Regelsatz und klicken Sie auf **Regelsatz bearbeiten**.
4. Klicken Sie auf **Neu**.
5. Wählen Sie in der Dropdown-Liste **Alarmtyp** die Komponente, Aktion oder den Ereignistyp aus, bei dem Sie alarmiert werden möchten.
6. Aktivieren Sie jeden Status, für den ein Alarm ausgelöst werden soll: **Zu Informationszwecken**, **OK**, **Warnung** oder **Kritisch**. Beispiel: Um einen Alarm zu erhalten, wenn der von Ihnen in Schritt 5 ausgewählte Typ einen kritischen Grenzwert überschreitet, wählen Sie **Kritisch**.
7. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, die ausgeführt werden soll, wenn die in Schritt 5 und 6 angegebenen Bedingungen eintreten. Diese Aktionen werden vorab definiert; wenn Sie eine Aktion initiierten möchten, die nicht in der Liste geführt wird, können Sie eine entsprechende Aktion erstellen. Verwenden Sie hierzu die Seite **Aktion-Regelsätze**.

   Hinweis: Bestimmte Alarme, die Computergruppen zugeordnet wurden, können simultan eine große Anzahl von Antworten generieren. Beispiel: Sie können den Alarm "Computerkonfiguration wurde geändert" konfigurieren und mit einer E-Mail-Aktion verknüpfen. Wenn ein Softwareverteilungs-Patch auf diejenigen Computer angewendet wird, die über diese Alarmeinstellung verfügen, würde dieses Patch eine ebenso große Anzahl von Core Server-E-Mails generieren wie Computer, auf die das Patch übertragen wurde. Das heißt, auf Ihre E-Mail-Server käme möglicherweise eine Flut von E-Mails zu. In diesem Fall besteht die Lösung möglicherweise darin, den Alarm ganz einfach in das Core-Protokoll zu schreiben, anstatt E-Mails zu senden.

8. Wählen Sie in der Dropdown-Liste **Alarmaktion** eine Konfiguration aus. Möglicherweise steht nur eine Konfiguration zur Verfügung (der Inhalt dieser Liste ändert sich, je nachdem, was Sie in Schritt 7 ausgewählt haben).
9. Aktivieren Sie das Kontrollkästchen **Hat Auswirkungen auf den Gerätezustand**, wenn Sie veranlassen möchten, dass der Alarm auf den Zustand des Servers angewendet wird, wenn dieser im in der Liste **Alle Geräte** angezeigt wird. Wenn der Schweregrad für den Alarm **Zu Informationszwecken** entspricht, wirkt sich der Alarm nicht auf den Gerätezustand aus.
10. Klicken Sie auf **Hinzufügen**.
11. Wiederholen Sie die Schritte 5-10, um zusätzliche Alarme zum Regelsatz hinzuzufügen.
12. Klicken Sie nach Eingabe aller erforderlichen Daten auf **Schließen**.

Um einen Alarmregelsatz zu bearbeiten, wählen Sie den Regelsatz aus (Schritt 3) und klicken Sie auf **Regelsatz bearbeiten**. Setzen Sie dann den Vorgang mit den oben aufgeführten Schritten fort.

Einige Minuten, nachdem Sie einen Regelsatz erstellt oder bearbeitet haben, versucht der Bereitstellungsdienst für Regelsätze automatisch, alle Computer, auf denen dieser Regelsatz zu einem früheren Zeitpunkt bereitgestellt worden war, zu aktualisieren. Wenn Sie den Regelsatz

sofort bereitstellen möchten, klicken Sie auf die Registerkarte **Regelsatz bereitstellen** und dann auf **Bereitstellen**.

Bereitstellen von Regelsätzen

Verwenden Sie die Seite **Regelsatz bereitstellen**, um den ausgewählten Alarmregelsatz auf Zielgeräte zu verschieben.

Bevor Sie einen Regelsatz auf einem verwalteten Gerät bereitstellen, müssen zuvor auf diesem Gerät ein Management-Agent installiert werden. Wenn Sie den Standard Management Agent bereitstellen, wird der Standardregelsatz bereitgestellt. Nachdem das Setup für den Agenten vollständig ausgeführt wurde, können Sie Regelsätze aktualisieren oder neue Regelsätze bereitstellen. Sie sollten zunächst die Zielgeräte auswählen, auf denen Sie den Alarmregelsatz bereitstellen möchten.

So stellen Sie einen Alarmregelsatz bereit

1. Klicken Sie im linken Navigationsfenster auf **Eigene Geräte** und dann auf die Gruppe **Alle Geräte**.
2. Wählen Sie die Geräte aus, auf denen Sie den Alarmregelsatz bereitstellen möchten, und klicken Sie dann auf **Ziel**, um die Geräte in die Liste **Zielgeräte** aufzunehmen.
3. Klicken Sie im linken Navigationsfenster auf **Alarmierung** und klicken Sie dann auf die Registerkarte **Regelsatz bereitstellen**.
4. Wählen Sie auf der Registerkarte **Alarmregelsätze** den Regelsatz aus, den Sie bereitstellen möchten.
5. Klicken Sie auf die Verknüpfung, um die Liste mit den Zielgeräten anzuzeigen. Wenn Sie ein Gerät aus dieser Liste löschen möchten, klicken Sie mit der rechten Maustaste auf das Gerät und klicken dann auf **Löschen**. Um alle Geräte zu entfernen, klicken Sie mit der rechten Maustaste auf einen beliebigen Gerätenamen und klicken dann auf **Zurücksetzen**. Um Geräte hinzuzufügen, müssen Sie sie der Zielliste hinzufügen (Schritte 1 - 2 oben).
6. Schließen Sie das Fenster **Zielliste** und klicken Sie dann auf **Bereitstellen**, um die ausgewählte Konfiguration auf den Zielgeräten bereitzustellen.

Als Teil des Bereitstellungsprozesses wird eine XML-Seite erstellt, die den bereitgestellten Regelsatz und die Geräte, auf denen der Regelsatz bereitgestellt wurde, auflistet. Dieser Bericht wird auf dem Core Server im Verzeichnis \ldlogon\alertrules gespeichert und mit einer fortlaufenden Nummer benannt, die ihm von der Datenbank zugewiesen wird. Wenn Sie diese XML-Seite unabhängig vom Bereitstellen eines Regelsatzes anzeigen möchten, klicken Sie auf die Schaltfläche **XML generieren** und klicken dann auf die Verknüpfung, mit der die XML-Datei angezeigt wird.

Beachten Sie, dass keine zwei benutzerdefinierten Regelsätze gleichzeitig auf einem verwalteten Gerät aktiv sein können. Wenn Sie einen benutzerdefinierten Regelsatz bereitgestellt haben und dann einen zweiten benutzerdefinierten Regelsatz auf demselben Gerät bereitstellen, wird der erste Regelsatz überschrieben und der zweite aktiviert.

Anzeigen von Alarm-Regelsätzen für ein Gerät

Verwenden Sie die Seite **Alarm-Regelsätze**, um eine Liste mit den Alarm-Regelsätzen einzublenden, die dem ausgewählten Gerät zugewiesen wurden; Sie können mit dieser Seite auch detaillierte Informationen zu den einzelnen Alarmen anzeigen.

So zeigen Sie Alarm-Regelsätze an

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten. In einem anderen Browser-Fenster wird die Serverinformationskonsole geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Regelsätze**.
3. Klicken Sie auf die Registerkarte **Regelsätze für die Alarmierung**.

Die folgenden Details werden zu jedem Regelsatz bereitgestellt. Weitere Informationen dazu, wie Sie diese Details ändern können, finden Sie unter Verwenden von Alarmen.

- **Wenn Status erreicht:** Wenn der Status des Alarms den angezeigten Status erreicht, wird ein Alarm ausgelöst.
- **Beeinflusst Zustand:** Gibt an, ob der Alarmstatus auf den Systemzustand des Servers angewendet wird, wenn er im Dashboard oder in der Liste Liste **Alle Geräte** angezeigt wird.
- **Regelsatz-Name:** Der Name des Alarm-Regelsatzes (entsprechend der Definition im Dialogfeld Alarm-Regelsätze).
- **Alarmtyp:** Eine Beschreibung der Alarmquelle (Hardware, Software, Ereignis etc.).
- **Aktionskonfiguration:** Die Aktion, die abläuft, wenn der Alarm generiert wird (entsprechend der Definition im Dialogfeld Aktionskonfigurationen.
- **Alarm-Handler:** Der zu generierende Alarmtyp, beispielsweise eine E-Mail, eine SNMP-Trap oder eine Programmausführung.
- **Instanz:** Gibt die genaue Quelle des Alarms an.

Sie können auch auf die Schaltfläche **Alarmprotokoll** klicken, um zum Alarmprotokoll des Geräts zu wechseln und Details zu Alarmen anzuzeigen. (Weitere Informationen finden Sie unter Anzeigen des Alarmprotokolls.)

Anzeigen des Alarmprotokolls

Verwenden Sie die Seite **Alarmprotokoll** zum Anzeigen von Alarmen, die an den Core (das globale Alarmprotokoll) oder an verwaltete Geräte gesendet wurden. Das Protokoll wird nach der Uhrzeit (GMT) sortiert, wobei sich die neuesten Einträge am Anfang des Protokolls befinden.

Das Alarmprotokoll enthält die folgenden Spalten:

- **Alarmname:** Der mit dem Alarm assoziierte Name - wie auf der Seite **Alarmkonfigurationen** definiert.
- **Uhrzeit:** Datum und Uhrzeit der Alarmerstellung (GMT).
- **Status:** Der Alarmstatus, wobei folgende Statusangaben unterstützt werden:

    - **Unbekannt:** Der Status lässt sich nicht ermitteln.
    - **Zu Informationszwecken:** Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen.
    - **OK:** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.
    - **Warnung:** Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
    - **Kritisch:** Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Instanz:** Gibt die genaue Quelle des Alarms an.
- **Gerätename:** Der Name des Geräts, auf dem der Alarm generiert wurde. Dies sollte ein vollständig qualifizierter Domänenname sein. (Nur globales Alarmprotokoll.)
- **IP-Adresse:** Die IP-Adresse des Geräts, auf dem der Alarm generiert wurde. (Nur globales Alarmprotokoll.)

Wenn der Gerätename nicht als vollständig qualifizierter Domänenname angezeigt wird, so liegt das daran, dass das Produkt nicht in der Lage war, den vollständig qualifizierten Domänennamen für das Gerät aufzulösen.

So zeigen Sie das globale Alarmprotokoll an

1. Klicken Sie im linken Navigationsfenster auf **Protokolle**.
2. Um Einträge nach Uhrzeit, Name, Status oder Instanz zu sortieren, klicken Sie auf eine Spaltenüberschrift.
3. Doppelklicken Sie auf den Eintrag in der Spalte **Alarmname**, um eine ausführliche Beschreibung des Alarms anzuzeigen.
4. Um Protokolleinträge nach Name, Status oder Instanz aufzulisten, wählen Sie die Filterkriterien in der Dropdown-Liste "Filter" aus. Wählen Sie beispielsweise **Alarmname** aus und geben Sie einen vollständigen Namen ein (beispielsweise "Performance"); oder geben Sie mit dem Platzhalter * einen Teil eines Namens ein (beispielsweise Remote*). Um einen Suchvorgang nach dem Datum auszuführen, wählen Sie **Datumsfilter aktivieren** aus, geben einen Bereich mit einem Anfangs- und Enddatum ein und klicken auf **Suchen**.
5. Um den Zustandsstatus eines Alarms zu löschen, wählen Sie den Alarm aus, indem Sie auf die Zahl in der Spalte **Alarmname** und dann auf **Alarm löschen** sowie anschließend auf **OK** klicken. Um einen Protokolleintrag zu löschen, wählen Sie den Alarm aus und klicken auf **Eintrag löschen**.
6. Um alle Einträge im Protokoll zu löschen, klicken Sie auf **Protokoll entfernen**.

So zeigen Sie das Alarmprotokoll für ein bestimmtes Gerät an

1. Doppelklicken Sie auf das Gerät in der Liste **Eigene Geräte**.
2. Klicken Sie im linken Navigationsfenster auf **Systeminformationen**.
3. Klicken Sie auf **Protokolle** und doppelklicken Sie dann auf **Alarmprotokoll**.
4. Um Einträge nach Uhrzeit, Name, Status oder Instanz zu sortieren, klicken Sie auf eine Spaltenüberschrift.
5. Klicken Sie auf den Eintrag in der Spalte **Alarmname**, um eine ausführliche Beschreibung des Alarms anzuzeigen.

6. Um Protokolleinträge nach Name, Status oder Instanz aufzulisten, klicken Sie auf die Schaltfläche **Filter** in der Symbolleiste und wählen Filterkriterien aus. Wählen Sie beispielsweise **Alarmname** aus und geben Sie einen vollständigen Namen ein (beispielsweise "Performance"); oder geben Sie mit dem Platzhalter * einen Teil eines Namens ein (beispielsweise Remote*). Klicken Sie dann auf "Suchen" in der Symbolleiste, um die Alarme anzuzeigen, die mit den von Ihnen ausgewählten Filteroptionen verknüpft sind.
7. Um Protokolleinträge für einen Datumsbereich anzuzeigen, deaktivieren Sie das Kontrollkästchen **Ereignisse für alle Daten anzeigen** und wählen einen Datumsbereich aus. Klicken Sie auf **Aktualisieren**, um Einträge für den betreffenden Datumsbereich anzuzeigen.

Software-Updates

System Manager beinhaltet ein Software-Updates-Tool, mit dem Sie nach Updates für Verwaltungs- und Betriebssystemsoftware sowie Gerätetreiber suchen können. Sie können diese Updates herunterladen und die betroffenen Geräte aktualisieren, indem Sie die relevanten Updates (auch Patches genannt) bereitstellen und installieren.

Dieses Kapitel befasst sich mit folgenden Themen:

Software-Updates - Übersicht

Mithilfe der Software-Updates-Tools können Sie sicherstellen, dass Ihre verwalteten Geräte netzwerkweit immer mit den neuesten Softwareversionen arbeiten. Sie können die sich wiederholenden Softwareaktualisierungsvorgänge und das Herunterladen sowie Installieren der erforderlichen Updates auf betroffenen Geräten automatisieren.

Der Zugriff auf das Software-Updates-Tool wird in diesem Produkt über das Standardmodell der rollenbasierten Administration gesteuert. Sie ist das Zugriffs- und Sicherheitsmodell des Produkts. Mithilfe der rollenbasierten Administration können Administratoren den Zugriff auf Tools und Geräte gezielt beeinflussen. Jedem Benutzer werden bestimmte Rechte und Bereiche zugewiesen, die festlegen, mit welchen Funktionen dieser Benutzer arbeiten und welche Geräte er verwalten kann. Ein Administrator weist diese Rechte anderen Benutzern zu (weitere Hinweise finden Sie unter Informationen zur rollenbasierten Administration). Um das Software-Updates-Tool verwenden zu können, muss der Benutzer mit den Rechten "Patch-Management", "einfache Webkonsole" und "Berichte" angemeldet sein.

Unterstützte Serverplattformen

Das Software-Updates-Tool unterstützt die meisten Standardplattformen für Server; das bedeutet, dass Sie auf verwalteten Servern nach Updates suchen und diese Updates auf verwalteten Servern bereitstellen können, die unter den folgenden Betriebssystemen laufen:

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4

- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional, Enterprise und Advanced)

Informationen zum Fenster "Software-Updates"

Benutzer mit dem Recht "Patch-Management" sehen das Tool **Software-Updates** im linken Navigationsfenster der Konsole. Wenn Sie auf **Software-Updates** klicken sehen Sie eine Symbolleiste und zwei Abschnitte in der rechten Seite des Fensters. Der linke Fensterausschnitt zeigt eine hierarchische Strukturansicht der Software-Update-Gruppen an. Klicken Sie auf eine Gruppe, um deren Inhalt im rechten Fensterausschnitt einzublenden. Im rechten Fensterausschnitt werden in einer Spalte Details zur Definition des Software-Updates angezeigt. Am oberen Rand befindet sich eine **Suchschaltfläche**, mit der Sie gezielt nach den angegebenen Kriterien suchen können. Folgende Zeichen des erweiterten Zeichensatzes werden im Feld **Suchen** nicht unterstützt: <, >, ', ", !.

Schaltflächen der Symbolleiste

- **Aktualisieren:** Öffnet das Dialogfeld **Anfälligkeitseinstellungen aktualisieren**. Sie können darin die Plattformen und Sprachen angeben, deren Software-Update-Informationen Sie aktualisieren möchten. Sie können außerdem festlegen, ob Updates in die Gruppe **Scannen** eingefügt und ob verknüpfte Patches gleichzeitig heruntergeladen werden sollen. Des Weiteren können Sie den Speicherort für heruntergeladene Patches und die Proxyserver-Einstellungen angeben.
- **Download planen:** Öffnet den Download-Task im Dialogfeld **Geplante Tasks**. Dort können Sie Taskoptionen konfigurieren. Wenn Sie auf **Speichern** klicken, wird der Download-Task in das Fenster **Geplante Tasks** eingefügt und auf der Registerkarte **Anfälligkeits-Task** angezeigt.
- **Patchtasks planen:** Öffnet das Dialogfeld **Anfälligkeitsscan planen**, in dem Sie einen Namen zur Verfügung stellen und Scanneroptionen konfigurieren können.
- **Aktualisieren:** Aktualisiert die Liste im rechten Fensterausschnitt mit den neuesten heruntergeladenen Update-Informationen.
- **Entfernen:** Öffnet das Dialogfeld **Sicherheits- und Patch-Definitionen entfernen**. Hier können Sie die Plattformen und Sprachen angeben, deren Anfälligkeitsinformationen Sie aus der Core-Datenbank entfernen möchten.

Linker Fensterausschnitt (Strukturansicht)

Im linken Fensterausschnitt werden folgende Gruppen angezeigt:

- **Scannen:** Führt alle Updates auf, nach denen gesucht wird, wenn das Software-Updates-Tools auf verwalteten Geräten ausgeführt wird. Mit anderen Worten: Wenn ein Update in dieser Gruppe vorhanden ist, wird es Teil des nächsten Scanvorgangs sein; ist es nicht enthalten, wird es nicht Teil des Scans sein.

  "Scannen" kann als ein möglicher Anfälligkeitszustand neben "Nicht scannen" und "Nicht zugewiesen" verstanden werden. Ein Software-Update kann immer nur in jeweils einer dieser drei Gruppen vorhanden sein. Ein Update wird mit einem eindeutigen Symbol, das dem jeweiligen Status entspricht (Fragezeichen (?) für "Nicht zugewiesen", rotes X für "Nicht scannen" und normales Anfälligkeitssymbol für "Scannen"), gekennzeichnet. Wenn Sie ein Update aus einer Gruppe in eine andere verschieben, ändert sich automatisch dessen Status.

  Um ein Software-Update aus einer Gruppe in eine andere zu verschieben, klicken Sie mit der rechten Maustaste auf das Update und wählen die Gruppe aus, in die das Update verschoben werden soll.

  Indem Sie Updates in die Gruppe "Scannen" verschieben, bestimmen Sie Art und Umfang des nächsten Software-Update-Scans.

  Neue Updates können während eines Aktualisierungsvorgangs auch automatisch der Gruppe "Scannen" hinzugefügt werden. Hierfür muss die Option **Neue Definitionen in die Gruppe "Scannen" einfügen** im Dialogfeld **Anfälligkeitseinstellungen aktualisieren** aktiviert werden.

  Wichtiger Hinweis zum Verschieben von Software-Updates aus der Gruppe "Scannen":
  Wenn Sie Software-Updates aus der Gruppe "Scannen" in die Gruppe "Nicht scannen" verschieben, werden die aktuellen Informationen, die darüber Auskunft geben, welche gescannten Geräte diese Updates erkannt haben, aus der Datenbank entfernt und stehen von nun an weder im Dialogfeld "Software-Updates-Eigenschaften" noch im Informationsdialogfeld des gescannten Servers zur Verfügung. Um diese Analyseinformationen wiederherzustellen, müssten Sie die Software-Updates wieder in die Gruppe "Scannen" verschieben und den Scan erneut ausführen.

- **Nicht scannen:** Führt die Software-Updates auf, nach denen beim nächsten Scannen der Geräte nicht gesucht wird. Wie oben bereits erwähnt, kann ein Update, das sich in der Gruppe "Nicht scannen" befindet, nicht auch gleichzeitig in der Gruppe "Scannen" oder "Nicht zugewiesen" enthalten sein. Sie können Updates in diese Gruppe verschieben, um sie auf einem Software-Update-Scan zu entfernen.

- **Erkannt:** Führt alle Software-Updates auf, die vom letzten Scan für alle Zielgeräte, die in diesem Scanauftrag eingeschlossen sind, erkannt wurden. Der Inhalt dieser Gruppe wird immer vom letzten Software-Update-Scan bestimmt und davon, ob ein Gerät oder mehrere Geräte gescannt wurden.

  Die Liste "Erkannt" ist eine Zusammenfassung aller erkannten Software-Updates, die beim jüngsten Scan gefunden wurden. Die Spalten "Gescannt" und "Erkannt" geben an, wie viele Geräte gescannt wurden und auf wie vielen davon das Software-Update erkannt wurde. Wenn Sie sich speziell informieren möchten, welche Server über ein erkanntes Update verfügen, klicken Sie mit der rechten Maustaste auf die Definition und wählen dann **Betroffene Computer anzeigen** aus. Beachten Sie, dass Sie Update-Informationen für einen bestimmten Server auch in dessen Dialogfeld Serverinformationskonsole anzeigen können.

  Software-Updates aus der Gruppe "Erkannt" können nur entweder in die Gruppe "Nicht zugewiesen" oder "Nicht scannen" verschoben werden.

- **Nicht zugewiesen:** Listet alle Software-Updates auf, die weder in die Gruppe "Scannen" noch "Nicht scannen" gehören. Die Gruppe "Nicht zugewiesen" ist im Wesentlichen ein Wartebereich für gesammelte Updates. Diese verbleiben dort, bis Sie entschieden haben, ob Sie auf diese Updates scannen möchten oder nicht.

  Standardmäßig werden gesammelte Software-Updates während eines Updates der Gruppe "Scannen" hinzugefügt.

  Sie können Software-Updates aus der Gruppe "Nicht zugewiesen" entweder in die Gruppe "Scannen" oder "Nicht scannen" verschieben.

- **Nach Betriebssystem anzeigen:** Listet alle heruntergeladenen Software-Updates auf, wobei die Informationen untergeordneten Gruppen zugeordnet werden, die dem jeweiligen Betriebssystem des Geräts entsprechen. Diese untergeordneten Gruppen helfen Ihnen, Updates nach Betriebssystemkategorie zu unterscheiden. Sie können die Betriebssystemuntergruppen verwenden, um einen Satz Updates zur Durchführung eines betriebssystemspezifischen Scanvorgangs in die Gruppe "Scannen" zu kopieren.

  Software-Updates können von einer Betriebssystemgruppe in die Gruppen "Scannen", "Nicht scannen" oder "Nicht zugewiesen" kopiert werden. Updates können in mehreren Plattform- und/oder Produktgruppen gleichzeitig vorkommen.

- **Nach Produkt anzeigen:** Liste alle heruntergeladenen Software-Updates nach Produktuntergruppen auf. Diese untergeordneten Gruppen helfen Ihnen, Updates nach Produktkategorie zu unterscheiden. Sie können diese Produktuntergruppen verwenden, um Updates für die Durchführung eines produktspezifischen Scanvorgangs in die Gruppe "Scannen" zu kopieren.

Rechter Fensterausschnitt (Listenansicht)

Im rechten Fensterausschnitt werden folgende Software-Update-Details in sortierbaren Spalten aufgelistet.

- **Kennung:** Gibt den eindeutigen, vom Anbieter definierten alphanumerischen Code des Updates an.
- **Schweregrad:** Gibt den Schweregrad des Updates an. Mögliche Schweregrade sind: "Service Pack", "Kritisch", "Hoch", "Mittel", "Niedrig", "Nicht anwendbar" und "Unbekannt".
- **Titel:** Kurze Beschreibung des Update-Typs und des Update-Ziels.
- **Sprache:** Gibt die Sprache des Betriebssystems an, das von dem Update betroffen ist.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem das Update vom Anbieter veröffentlicht wurde.
- **Unbeaufsichtigte Installation:** Gibt an, ob die mit dem Update verbundene Patch-Datei unbeaufsichtigt (ohne Benutzerbeteiligung) installiert wird. Einige Updates können mit mehreren Patches verbunden sein. Wenn ein Update-Patch nicht unbeaufsichtigt installiert werden kann, gibt das Attribut "Unbeaufsichtigte Installation" des Updates "Nein" zurück.
- **Reparierbar:** Gibt an, ob sich das Update durch Bereitstellung und Installation einer Patch-Datei reparieren lässt. Zu den möglichen Werten gehören: "Ja", "Nein", "Einige" (für ein Update, das mehrere Erkennungsregeln einschließt, und wenn nicht alle erkannten Updates repariert werden können).

Doppelklicken Sie auf die Update-Kennung, um ausführliche Informationen im Dialogfeld "Eigenschaften" des Updates anzuzeigen. Im Dialogfeld "Eigenschaften" eines Updates können Sie die Erkennungsregeln für das Update anzeigen, verknüpfte Patch-Dateien herunterladen und auf die Regel klicken, um deren detaillierte Eigenschaften in einem entsprechenden Dialogfeld anzuzeigen.

Konfigurieren von Geräten für das Scannen auf Software-Updates

Damit verwaltete Geräte auf Anfälligkeiten gescannt werden und Patch-Verteilungen erhalten können, muss auf ihnen der Software-Updates-Agent installiert sein.

Die einfachste Methode, den Software-Updates-Agent auf mehreren verwalteten Geräten bereitzustellen, besteht darin, eine neue Agentenkonfiguration zu erstellen, in der der Software-Updates-Agent ausgewählt ist (Standardeinstellung), und dann den Konfigurationsvorgang für die gewünschten Zielgeräte mit dem Tool **Geplante Tasks** zu planen.

Wenn Sie ein Gerät für die Unterstützung von Software-Updates konfigurieren, werden die für das Software-Update-Scannen und -Reparieren (d.h. Patch-Bereitstellung und -Installation) benötigten Dateien auf dem Zielgerät installiert.

Aktualisieren von Software-Update-Definitionen

Was das Thema "Wartung" betrifft (d.h. die sichere Implementierung von Software-Updates und Bug Fixes), ist Ihr Netzwerk ständig verletzbar. Das Software-Updates-Tool vereinfacht und beschleunigt den Prozess des Sammelns der jeweils neuesten Patch-Informationen, indem es Ihnen die Möglichkeit gibt, Ihre Softwareprodukte über eine LANDesk-gehostete Datenbank zu aktualisieren. Dieser Dienst konsolidiert Updates, die von vertrauenswürdigen Branchen-/Anbieterquellen veröffentlicht werden.

Durch das Sammeln und Warten von Up-to-Date-Patch-Informationen gewinnen Sie einen besseren Überblick darüber, welche Software-Updates in welchem Umfang für die einzelnen

Serverbetriebssysteme Ihres Unternehmens benötigt werden. Der erste Schritt besteht darin, immer über die neuesten bekannt gewordenen Update-Informationen zu verfügen.

Sie können Software-Updates bei Verfügbarkeit sofort konfigurieren und ausführen oder Sie können einen Update-Task planen, der zu einem von Ihnen festgelegten Zeitpunkt oder als wiederkehrender Task ausgeführt wird.

So aktualisieren Sie Software-Update-Informationen

1. Klicken Sie im linken Navigationsfenster auf **Software-Updates**. (Eine Beschreibung dieses Dialogfelds finden Sie unter Das Fenster "Software-Updates".)
2. Klicken Sie auf die Schaltfläche **Update** in der Symbolleiste.
3. Wählen Sie in der Liste der verfügbaren Content-Server die Download-Quelle aus.
4. Wählen Sie die Plattformen aus, deren Software-Update-Informationen Sie aktualisieren möchten. Sie können eine oder mehrere Plattformen aus der Liste wählen. Je mehr Plattformen Sie auswählen, umso länger dauert die Aktualisierung.
5. Wählen Sie die Sprachen, deren Software-Update-Informationen Sie für die von Ihnen angegebenen Plattformen aktualisieren möchten. Sie können eine oder mehrere Sprachen aus der Liste auswählen. Je mehr Sprachen Sie auswählen, umso länger dauert die Aktualisierung.
6. Wenn Sie veranlassen möchten, dass neue Software-Update-Definitionen (Anfälligkeiten, die noch nicht in der Datenbank existieren) automatisch in die Gruppe "Nicht zugewiesen" anstatt in den Standardspeicherort (Gruppe "Scannen") eingefügt werden, deaktivieren Sie das Kontrollkästchen **Neue Definitionen in die Gruppe "Scannen" einfügen**.
7. Wenn Sie die aktuellen ausführbaren Patch-Dateien automatisch herunterladen möchten, aktivieren Sie das Kontrollkästchen **Patches für oben ausgewählte Definitionen herunterladen** und klicken anschließend auf eine der Download-Optionen.

    - **Nur für erkannte Definitionen:** Es werden nur die Patches heruntergeladen, die mit Software-Updates verknüpft sind, die beim letzten Software-Update-Scan erkannt wurden (z.B. die Updates, die sich derzeit in der Gruppe "Erkannt" befinden).
    - **Für alle referenzierten Definitionen:** Es werden ALLE Patches heruntergeladen, die mit Software-Updates verknüpft sind, die sich derzeit in der Gruppe "Scannen" befinden. (dieser Vorgang ist mit einem hohen Zeitaufwand verbunden)

    Die Patches werden in den Speicherort heruntergeladen, der im Abschnitt "Patch-Einstellungen" des Dialogfelds angegeben wurde (siehe unten beschriebenen Vorgang).
8. Wenn in Ihrem Netzwerk ein Proxyserver installiert ist, der für externe Internet-Übertragungen verwendet wird (zum Aktualisieren von Update-Informationen und Herunterladen von Patches erforderlich), klicken Sie auf die Registerkarte **Proxyeinstellungen** und aktivieren das Kontrollkästchen **Proxyserver verwenden**. Geben Sie die Adresse, Anschlussnummer und Anmeldeinformationen für die Authentifizierung des Servers an, falls der Zugriff auf den Proxyserver per Anmeldevorgang erfolgt.
9. Klicken Sie auf **Übernehmen**, wenn Sie die Einstellungen speichern möchten.
10. Klicken Sie auf **Jetzt aktualisieren**, um das Software-Update auszuführen. Das Dialogfeld **Sicherheits- und Patch-Definitionen aktualisieren** zeigt den aktuellen Vorgang und Status an.

11. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Schließen**. Wenn Sie auf **Abbrechen** klicken, bevor das Update abgeschlossen ist, werden nur die bis zu diesem Zeitpunkt verarbeiteten Software-Update-Informationen in die Core-Datenbank geladen. Sie müssen die Aktualisierung erneut ausführen, um alle restlichen Informationen abzurufen.

Hinweis: Schließen Sie die Konsole nicht, während eines Updates, da der Prozess andernfalls beendet wird. Dies gilt nicht für einen geplanten Download-Task.

Wenn Sie LANDesk® Management Suiteund System Manager auf demselben Core Server installiert haben, verwenden beide Produkte dieselben Einstellungen, um festzustellen, welche Anfälligkeitstypen aktualisiert werden. In einigen Fällen werden möglicherweise Updates in Management Suite angezeigt, die nur von System Manager aus beim Ausführen des Updates konfigurierbar sind. Beispiel: Wenn Sie "Sicherheitsbedrohungen" als eine Update-Option in System Manager ausgewählt haben und dann beschließen, Software-Updates in System Manager zu aktualisieren, werden beim Ausführen des Updates in Management Suite sowohl die Software-Updates als auch die Sicherheitsbedrohungen in den aktualisierten Elementen angezeigt.

So konfigurieren Sie den Speicherort für das Patch-Download

1. Klicken Sie im Dialogfeld **Anfälligkeitseinstellungen aktualisieren** auf die Registerkarte **Patch-Einstellungen**.
2. Geben Sie einen UNC-Pfad für die kopierten Patch-Dateien an. Der Standardspeicherort ist das Verzeichnis \LDLogon\Patch des Core Servers.
3. Wenn der oben eingegebene UNC-Pfad auf einen anderen Speicherort als den Core Server zeigt, geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort ein, um eine Authentifizierung gegenüber diesem Speicherort durchzuführen.

   Für den Ordner müssen Datei- und Webfreigabe sowie "Anonymer Zugriff" aktiviert sein.

4. Geben Sie eine Web-URL-Adresse ein, über die Server auf die heruntergeladenen Patches für die Verteilung zugreifen können. Die Web-URL-Adresse sollte dem oben angegebenen UNC-Pfad entsprechen.
5. Sie können auf **Testeinstellungen** klicken, um zu prüfen, ob mit der oben angegebenen Web-Adresse eine Verbindung hergestellt werden kann.
6. Wenn Sie den UNC-Pfad und die Web-URL wieder auf die Standardeinstellung für den Speicherort zurücksetzen möchten, klicken Sie auf **Patch-Einstellungen zurücksetzen**. Der Standardspeicherort ist das Verzeichnis \LDLogon\Patch des Core Servers.

Festlegen von Zeitplänen für Software-Updates

Sie können Software-Updates auch als geplanten Task konfigurieren, der automatisch zu einem festgelegten Zeitpunkt oder wiederkehrend ausgeführt wird. Hierfür müssen Sie lediglich in der Symbolleiste auf die Schaltfläche **Download planen** klicken, um das Dialogfeld **Geplanter Task - Eigenschaften** zu öffnen, dem Task einen Namen zuzuweisen und dessen Optionen zu konfigurieren. Beim Klicken auf **Speichern** wird der Task im Fenster "Geplante Tasks" angezeigt.

Alle geplanten Software-Update-Tasks verwenden die aktuellen Einstellungen aus dem Dialogfeld **Anfälligkeitseinstellungen aktualisieren**. Wenn Sie die Einstellungen für die

Website-Quelle, Plattformen, Sprachen, Patch-Downloads oder Proxy-Server für einen bestimmten Aktualisierungsauftrag ändern möchten, müssen Sie diese Einstellungen zuerst im Dialogfeld **Anfälligkeitseinstellungen aktualisieren** ändern, und zwar vor dem geplanten Ausführungszeitpunkt des Tasks.

So konfigurieren Sie den Task "Download planen"

1. Klicken Sie im linken Navigationsfenster auf **Software-Updates**.
2. Klicken Sie auf **Download planen**.
3. Konfigurieren Sie auf der Seite **Task planen** den Zeitplan.
4. Klicken Sie auf **Speichern**.

Wenn Sie auf **Download planen** klicken, wird ein Task erstellt (er verfügt über keine Zielgeräte und keinen Zeitplan). Wenn Sie die Prozedur für den **geplanten Task** abbrechen, sollten Sie beachten, dass der Task dennoch erstellt wurde und in der Liste **Eigene Tasks** angezeigt wird.

Anzeigen von Informationen zu Software-Updates und Erkennungsregeln

Nachdem Software-Updates mit den neuesten Informationen aus dem LANDesk-Sicherheitsdienst aktualisiert wurden, können Sie Software-Update-Listen in der Konsole und nach Plattform und Produkt sortiert anzeigen sowie die Updates in verschiedene Statusgruppen verschieben. Weitere Informationen zu den verschiedenen Gruppen in diesem Fenster und zu deren Verwendung finden Sie unter Informationen zum Fenster "Software-Updates" weiter oben in diesem Kapitel.

Um detaillierte Informationen zu einem Software-Update einzublenden, doppelklicken Sie auf eine Software-Updates-ID, um das zugehörige Dialogfeld "Eigenschaften" zu öffnen. Von diesem Dialogfeld aus können Sie auch auf die Details von Erkennungsregeln zugreifen, indem Sie durch Doppelklicken auf den Namen einer Patch-Datei in der Liste Erkennungsregeln das Dialogfeld "Patch-Eigenschaften" öffnen (siehe Informationen zum Dialogfeld "Patch-Eigenschaften").

Anhand dieser Informationen können Sie bestimmen, welche Updates für die von Ihrem Netzwerk unterstützten Serverplattformen relevant sind, wie die Erkennungsregeln eines Updates ein Update ausfindig machen, welche Patches verfügbar sind und wie Sie die Sanierungsmaßnahmen für die betroffenen Geräte konfigurieren und ausführen sollten.

Außerdem können Sie direkt von der Konsole aus gezielt (auf gescannte Geräte bezogene) Informationen zur Software-Update-Definition und zu Erkennungsregeln anzeigen, indem Sie über **Eigene Geräte** auf die Serverinformationskonsole zugreifen und auf **Software-Updates** im linken Navigationsfenster klicken.

Entfernen von Software-Update-Informationen

Sie können Software-Update-Informationen aus dem Fenster "Software-Updates" (und anschließend aus der Core-Datenbank) löschen, wenn Sie feststellen, dass diese Informationen für Ihre Umgebung nicht von Belang sind.

Beim Löschen von Software-Update-Informationen werden auch die zugehörigen Erkennungsregelinformationen aus der Datenbank entfernt. Die eigentlichen ausführbaren Patch-

Dateien werden bei diesem Vorgang jedoch nicht entfernt. Die Patch-Dateien müssen manuell aus der lokalen Ablage gelöscht werden, die sich in der Regel auf dem Core Server befindet.

So entfernen Sie Software-Update-Informationen

1. Klicken Sie auf die Schaltfläche **Entfernen** in der Symbolleiste. (Eine Beschreibung dieses Dialogfelds finden Sie unter Informationen zum Dialogfeld "Sicherheit und Patch-Definitionen entfernen").
2. Wählen Sie die Plattformen aus, deren Software-Update-Informationen Sie entfernen möchten. Sie können eine oder mehrere Plattformen in der Liste auswählen.

   Wenn ein Update mit mehreren Plattform verknüpft ist, müssen Sie alle verknüpften Plattformen auswählen, da andernfalls die Informationen zum Update nicht entfernt werden.

3. Wählen Sie die Sprachen aus, deren Update-Informationen Sie entfernen möchten (mit der oben angegebenen Plattform verknüpft).

   Wenn Sie oben eine Windows-Plattform auswählen, sollten Sie angeben, welche sprachenbezogenen Update-Informationen Sie entfernen möchten.. Haben Sie oben eine UNIX-Plattform ausgewählt, dann müssen Sie die Option "Sprache neutral" angeben, damit die sprachübergreifenden Update-Informationen gelöscht werden.

4. Klicken Sie auf **Entfernen**.

Scannen auf Software-Updates

Mit "Software-Update-Analyse" ist gemeint, dass die auf einem Gerät aktuell installierten Versionen betriebssystemspezifischer Dateien und Registrierungsschlüssel auf die neuesten bekannten Software-Updates überprüft werden, um den Update-Bedarf Ihrer Server zu ermitteln. Nachdem Sie bekannte Software-Update-Informationen (aktualisiert mit Informationen aus den relevanten Quellen der Branche) durchgesehen und entschieden haben, nach welchem Update gescannt werden muss, können Sie auf verwalteten Geräten, auf denen der Software-Updates-Agent installiert ist, eine benutzerdefinierte Analyse durchführen. (Weitere Informationen zum Konfigurieren von Geräten für Scanvorgänge und für die Patch-Bereitstellung finden Sie unter Konfigurieren von Geräten für das Scannen auf Software-Updates weiter oben in diesem Kapitel.)

Wenn der Anfälligkeitsscanner ausgeführt wird, liest er die Einträge der Gruppe "Scannen" und sucht nach diesen speziellen Updates. Bevor Sie Server auf Updates scannen, sollten Sie stets sicherstellen, dass nur die Software-Updates, auf die Sie scannen möchten, in dieser Gruppe enthalten sind. Sie können Software-Updates jederzeit manuell in die Gruppe "Scannen" verschieben oder daraus entfernen, um Größe und Art eines Scans anzupassen.

Ausführen des Software-Updates-Scanners

Der Software-Updates-Scanner kann mit einem Push-Verfahren als geplanter Scan-Task von der Konsole aus auf Geräten bereitgestellt werden.

So erstellen Sie einen Task für die Durchführung eines Software-Updates-Scan

1. Klicken Sie im linken Navigationsfenster auf **Software-Updates**.
2. Stellen Sie sicher, dass die Software-Update-Definitionen in jüngster Zeit aktualisiert wurden.
3. Stellen Sie sicher, dass die Gruppe "Scannen" nur diejenigen Updates enthält, auf die Sie scannen möchten.
4. Klicken Sie auf die Symbolleistenschaltfläche **Patchtasks planen**. (Eine Beschreibung dieses Dialogfelds finden Sie unter "Informationen zum Dialogfeld 'Anfälligkeitsscan planen'".)
5. Geben Sie einen eindeutigen Namen für den Scan ein. Wenn das Skript für den Task bereits existiert, können Sie angeben, ob das vorhandene Skript überschrieben werden soll.
6. Geben Sie an, ob der Software-Updates-Scanner auf dem Zielgerät ein Dialogfeld zum Scanverlauf anzeigen soll. Sie können auch angeben, ob eine Schaltfläche zum Abbrechen des Vorgangs zusammen mit dem Scanner-Dialogfeld angezeigt werden soll, sodass der Endanwender die Möglichkeit erhält, den Scan zu stornieren.
7. Geben Sie an, wie das Dialogfeld des Software-Updates-Scanners geschlossen werden soll, wenn die Ausführung auf den Zielgeräten beendet ist. Sie können Benutzereingaben zur Bedingung machen oder das Dialogfeld so konfigurieren, dass es nach einem angegebenen Timeout automatisch geschlossen wird.
8. Klicken Sie auf **OK**.
9. Wählen Sie den Task im unteren Fensterbereich aus (unter **Anfälligkeits-Tasks**) und klicken Sie auf **Bearbeiten**. Legen Sie Ziel- und Zeitplanparameter fest und klicken Sie auf **Speichern**.

Anzeigen erkannter Updates

Wenn der Software-Updates-Scanner auf einem der Zielgeräte Updates für eines der aktivierten Software-Updates findet, wird diese Information an den Core Server weitergegeben und in die Liste **Erkannt** geschrieben.

Nach der Durchführung eines Software-Updates-Scan können Sie mit einer der folgenden Methoden erkannte Updates anzeigen:

Nach der Gruppe "Erkannt"

Wählen Sie die Gruppe **Erkannt** im Fenster "Software-Updates" aus, um eine vollständige Liste aller Updates einzublenden, die während des letzten Scans erkannt wurden.

Nach einem einzelnen Gerät

Doppelklicken Sie auf einen Gerätenamen in der Liste **Eigene Geräte** und klicken Sie dann auf **Software-Updates**, um detaillierte Informationen zur Software-Update-Analyse für das betreffende Gerät anzuzeigen.

Herunterladen von Patches

Damit Patches auf Geräten mit erkannten Software-Updates bereitgestellt werden können, muss die Patch-Programmdatei in einen lokalen Patch-Pool in Ihrem Netzwerk heruntergeladen werden. Als Standardspeicherort für Patch-Downloads ist das Verzeichnis "/LDLogon" auf dem Core Server vorgegeben. Sie können diesen Speicherort im Abschnitt **Patch-Einstellungen** des Dialogfelds **Anfälligkeitseinstellungen aktualisieren** ändern.

Einstellungen zu Speicherort und Proxy-Server für Patch-Downloads
Patch-Downloads verwenden immer die aktuellen Einstellungen für den Download-Speicherort aus dem Abschnitt **Patch-Einstellungen** des Dialogfelds **Anfälligkeitseinstellungen aktualisieren**. Beachten Sie außerdem, dass Sie vor dem Herunterladen von Patch-Dateien die Einstellungen für den Proxyserver im Abschnitt **Proxyeinstellungen** des Dialogfelds **Anfälligkeitseinstellungen aktualisieren** entsprechend konfigurieren müssen, falls Ihr Netzwerk einen Proxyserver für den Internet-Zugang verwendet.

Das Produkt versucht zuerst, Patch-Dateien von der im Dialogfeld "Patch-Eigenschaften" angezeigten URL herunterzuladen. Falls keine Verbindung hergestellt werden kann oder das Patch aus irgendeinem Grund nicht verfügbar ist, lädt das Produkt das Patch vom LANDesk-Sicherheitsdienst herunter, d.h. aus einer Datenbank des Unternehmens, die Patches aus vertrauenswürdigen Quellen der Branche enthält.

Sie können jedes Patch einzeln oder mehrere Patches gleichzeitig herunterladen.

So laden Sie einzelne Patches herunter

1. Klicken Sie auf den Namen eines Software-Updates, um das Dialogfeld **Eigenschaften** für dieses Update zu öffnen.
2. Wählen Sie im Abschnitt **Erkennungsregeln** die Patch-Dateien aus, die Sie für die Erkennungsregeln herunterladen möchten, und klicken Sie dann auf **Ausgewählte Patches herunterladen**.
3. Informationen zum Download-Vorgang und –Status werden im Dialogfeld **Patches werden heruntergeladen** angezeigt. Sie können jederzeit auf **Abbrechen** klicken, um den gesamten Download-Vorgang zu stoppen.
4. Wenn der Download beendet ist, klicken Sie auf die Schaltfläche **Schließen**.

So laden Sie mehrere Patches herunter

Alle geplanten Software-Update-Tasks verwenden die aktuellen Einstellungen aus dem Dialogfeld **Anfälligkeitseinstellungen aktualisieren**. Wenn Sie die Einstellungen für die Website-Quelle, Plattformen, Sprachen, Patch-Downloads oder Proxy-Server für einen bestimmten Aktualisierungsauftrag ändern möchten, müssen Sie diese Einstellungen zuerst im Dialogfeld **Anfälligkeitseinstellungen aktualisieren** ändern, und zwar vor dem geplanten Ausführungszeitpunkt des Tasks.

1. Klicken Sie im linken Navigationsfenster auf **Software-Updates**.
2. Klicken Sie auf **Download planen**.
3. Konfigurieren Sie auf der Seite **Task planen** den Plan für die Ausführung des Tasks.
4. Klicken Sie auf **Speichern**.

Entfernen von Patch-Dateien

Um Patch-Dateien zu entfernen, müssen Sie die Dateien manuell aus der Patch-Ablage löschen, die sich für gewöhnlich im LDLogon-Verzeichnis des Core Servers befindet.

Reparieren von Software-Updates

Nachdem Sie die Software-Update-Informationen aktualisiert, die Updates, auf die Sie scannen möchten, in die Gruppe "Scannen" eingefügt, einen Scan auf verwalteten Geräten ausgeführt und entschieden haben, welchen Software-Updates Sie Ihre Aufmerksamkeit schenken müssen, sowie die erforderlichen Patches heruntergeladen haben, besteht der nächste Schritt darin, Software-Updates durch Bereitstellung und Installation der relevanten Patches auf betroffenen Geräten zu reparieren.

Software-Update-Reparaturen werden einzeln für jedes Software-Update ausgeführt. Das heißt, Sie erstellen einen Reparaturtask, der die erforderlichen Patch-Dateien für das betroffene Software-Update bereitstellt und installiert.

Beachten Sie, dass das Reparieren von Software-Updates, ähnlich wie das Software-Update-Scannen, sich nur auf Geräten durchführen lässt, die mit dem Software-Updates-Agenten konfiguriert wurden. Weitere Informationen finden Sie unter Konfigurieren von Geräten für das Scannen auf Software-Updates weiter oben in diesem Kapitel.

Linux-Reparatur wird unterstützt. Sie können das Tool "Software-Updates" verwenden, um Anfälligkeiten auf Linux-Geräten zu erkennen, und dann entscheiden, ob Sie die Updates reparieren möchten. Wenn Sie dies tun möchten, können Sie mit einem Supportabonnement Ihres Linux-Anbieters die erforderlichen RPMs herunterladen und dann die RPMs auf Geräten bereitstellen.

Warnung: Viele Patches starten automatisch das Gerät neu, nachdem sie ausgeführt wurden.

So erstellen Sie ein benutzerdefiniertes Reparaturskript

1. Klicken Sie im linken Navigationsfenster auf **Software-Updates**.
2. Wählen Sie die Gruppe **Erkannt**, um Software-Updates einzublenden, die vom letzten Scan erkannt wurden. (Sie müssen diese Gruppe nicht auswählen. Wenn Sie ein benutzerdefiniertes Reparaturskript erstellen möchten für Updates, auf die noch nicht gescannt wurde oder die noch nicht erkannt wurden, klicken Sie auf eine der anderen Anfälligkeitsgruppen, um deren Inhalt anzuzeigen und eine bestimmte Anfälligkeit auszuwählen.)
3. Klicken Sie mit der rechten Maustaste auf die Definition und wählen Sie dann **Betroffene Geräte anzeigen**, um Geräte anzuzeigen, die von diesem Software-Update betroffen sind.
4. Klicken Sie mit der rechten Maustaste auf die Definition und wählen Sie dann **Remediation-Task erstellen** aus.
5. (Optional) Ändern Sie den Namen im Textfeld **Taskname**.
6. Wählen Sie eine Option aus und klicken Sie auf **OK**.
    - **Kopieren Sie betroffene Computer in den Zielwagen:** Kopiert vom Software-Update betroffene Computer zum Reparieren in den Zielwagen.

- **Während der Ausführung Fortschritt anzeigen:** Ermöglicht es dem Scanner, während der Ausführung auf Endanwendergeräten Informationen einzublenden. Klicken Sie auf diese Option, wenn Sie Scanneraktivitäten einblenden und andere Anzeige- und Interaktionsoptionen in diesem Dialogfeld konfigurieren möchten. Wenn Sie nicht auf diese Option klicken, wird keine der anderen Optionen in diesem Dialogfeld für den Konfigurationsvorgang zur Verfügung gestellt und der Scanner transparent auf Geräten ausgeführt.
- **Benutzereingabe vor dem Schließen des Dialogfelds "Anfälligkeitsscan" erforderlich.** Klicken Sie auf diese Option, wenn der Scanner auf dem Bildschirm des Endanwenders eine Eingabeaufforderung einblenden soll, bevor das Scanner-Dialogfenster auf dem Gerät geschlossen wird. Wenn Sie diese Option auswählen und der Endanwender nicht reagiert, bleibt das Dialogfeld geöffnet. Das kann Zeitüberschreitungskonflikte mit anderen geplanten Tasks verursachen.
- **Dialogfeld nach einer Zeitüberschreitung automatisch schließen:** Klicken Sie auf diese Option, wenn Sie veranlassen möchten, dass das Dialogfenster des Scanners nach dem von Ihnen angegebenen Zeitraum geschlossen wird.

Skripte

Verwalten von Skripten

Dieses Produkt verwendet Skripte zum Ausführen benutzerdefinierter Tasks auf Geräten. Beim Auswählen von Optionen in den Dialogfeldern für die Skripterstellung wird eine ASCII-Textdatei im Windows INI-Format mit einer .INI-Erweiterung angelegt. Diese Skripte werden auf dem Core Server im Ordner \Programme\LANDesk\ManagementSuite\Scripts gespeichert. Der Dateiname des Skripts entspricht dem Namen des Skripts in der Konsole. Sie können lokale Scheduler-Skripte für Windows-Geräte mithilfe des Fensters **Skripte** erstellen (im linken Navigationsbereich auf **Skripte** klicken), oder Sie können eigene Skriptdateien schreiben und im Skriptordner speichern.

Das Fenster **Skripte** ordnet Skripte den folgenden Kategorien zu:

- **Eigene Skripte:** Skripte, die Sie mit dieser Gruppe verknüpfen.
- **Alle anderen Skripte:** Alle Skripte auf dem Core Server.
- **Benutzerskripte** (nur für Administratoren sichtbar): Von allen Benutzern des Produkts erstellte Skripte. Diese werden nach Skriptersteller sortiert.

Sie können Gruppen unter dem Objekt **Eigene Skripte** erstellen, um Ihre Skripte noch differenzierter zu unterteilen. Um ein neues lokales Scheduler-Skript zu erstellen, klicken Sie auf die Schaltfläche **Lokal**.

Nachdem Sie ein Skript erstellt haben, können Sie im Kontextmenü des Skripts auf **Planen** klicken. Im Fenster **Eigene Geräte** können Sie Zielgeräte auswählen, auf denen der Task ausgeführt werden soll; darüber hinaus können Sie angeben, wann der Task vom Fenster **Geplante Tasks** aus ausgeführt werden soll. Lesen Sie den Abschnitt "Tasks planen" um weitere Informationen zur Taskplanung zu erhalten.

Änderungen des Skript- und Taskeigentümers für Benutzer früherer Management Suite Versionen

In den 8.70 Versionen vor Management Suite waren alle Skripte global und für alle Benutzer sichtbar. Jetzt können Skripte nur noch vom Skriptersteller und von den Administratoren angezeigt werden.

Das Fenster **Skripte** verfügt über eine Spalte mit der Bezeichnung "Status". Die Spalte "Status" zeigt "Öffentlich", wenn alle Benutzer das Skript sehen können, oder "Privat", wenn nur der Benutzer, der das Skript erstellt hat, das Skript sehen kann. Benutzer können mit der rechten Maustaste auf von ihnen erstellte Skripte klicken, und sie können auf "Privat" oder "Öffentlich" klicken, um den Status eines Skripts zu ändern. Administratoren können den Status eines jeden Skripts ändern.

DOS PE ist die Standardumgebung. Wenn Sie eine andere Preboot-Umgebung auswählen, können Sie kein Befehlsskript erstellen. Für Windows- und Linux PEs können Sie nur auf Aufzeichnungs- oder Bereitstellungsskript generieren.

Wenn Sie Linux PE auswählen, verfügen Sie nur über die Imaging-Tool-Optionen LANDesk oder "Sonstige". Wenn Sie Windows PE auswählen, stehen Ihnen LANDesk, Sonstige und Microsoft* XImage zur Verfügung.

Erstellen eines Local Scheduler-Skripts

Der Local Scheduler ist ein Dienst, der auf Geräten ausgeführt wird. Er wird installiert, wenn Sie eine Agentenkonfiguration als Teil des Standard Management Agent bereitstellen. Im Allgemeinen verwaltet der Local Scheduler Produktaufgaben, beispielsweise die regelmäßige Ausführung des Inventarscanners. Andere zeitplangesteuerte Tasks, z. B. Software- oder Betriebssystembereitstellungen

Der Local Scheduler weist jedem Task eine Kennnummer zu. Der Kennungsbereich der lokalen Scheduler-Skripte unterscheidet sich von den Standardskripten des Local Schedulers, mit denen das Produkt arbeitet. Auf jedem Gerät darf immer nur ein benutzerdefiniertes Scheduler-Skript aktiv sein. Wenn Sie ein neues Skript erstellen und auf Geräten bereitstellen, ersetzt das neue Skript das alte Skript (jedes Skript im benutzerdefinierten Kennungsbereich des Local Schedulers), ohne sich auf die Standardskripte des Local Schedulers (beispielsweise den Zeitplan für den lokalen Inventarscan) auszuwirken.

Beim Auswählen von Zeitplanoptionen für das Skript sollten Sie die Einschränkungen der jeweiligen Optionen berücksichtigen. Wenn Sie z.B. als Wochentag den Montag auswählen und den 17. als Tag des Monats, wird der Task nur an einem Montag ausgeführt, der auch gleichzeitig der 17. des Monats ist; dieser Fall tritt jedoch nur sehr selten ein.

Sie können ein Skript erstellen, mit dem "restartmon.exe" auf einem lokalen Rechner - entweder sofort oder zu jedem anderen gewünschten Zeitpunkt - ausgeführt wird. Wenn Sie den Eindruck haben, dass die Berichterstellung von einem bestimmten Rechner gestoppt wurde, können Sie mithilfe von "restartmon.exe" im Ordner LDClient den Collector und alle Überwachungsanbieter neu starten. Dieses Dienstprogramm ist für Rechner gedacht, auf denen die Berichterstellung installiert wurde, jedoch keine Berichte mehr erstellt werden. Starten Sie mit diesem Dienstprogramm die Collector und Provider neu, ohne das Gerät neu starten zu müssen.

1. Klicken Sie im linken Navigationsfenster auf **Skripte**.
2. Klicken Sie auf **Lokal**.
3. Geben Sie einen Skriptnamen ein.
4. Klicken Sie auf **Hinzufügen**, um die Optionen für das Skript zu definieren.
5. Konfigurieren Sie die Local Scheduler-Optionen wie bereits beschrieben. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.
6. Klicken Sie auf **Speichern**, um Ihr Skript zu speichern.
7. Wählen Sie das Skript in der Gruppe **Eigene Skripte** aus, und klicken Sie dann auf **Planen**, um das von Ihnen erstellte Skript auf Geräten bereitzustellen.

Erläuterungen zu den Bandbreitenoptionen

Beim Konfigurieren von Local Scheduler-Befehlen können Sie angeben, wie viel Bandbreite das verwaltete Gerät mindestens bereitstellen muss, damit der Task ausgeführt wird. Zu dem Zeitpunkt, zu dem der Task ausgeführt werden soll, sendet jedes Gerät, das den Local Scheduler-Task ausführt, eine kleine Menge ICMP-Netzwerkdaten an den von Ihnen angegebenen Computer und wertet die Übertragungsleistung aus. Wenn der Zielcomputer für den Test nicht verfügbar ist, wird der Task nicht ausgeführt.

Sie können folgende Bandbreitenoptionen auswählen:

- **RAS:** Der Task wird ausgeführt, wenn die Netzwerkverbindung des Geräts mit dem Zielcomputer mindestens RAS- oder DFÜ-Geschwindigkeit erreicht. Diese Option auszuwählen bedeutet im Allgemeinen, dass der Task immer ausgeführt wird, wenn das Gerät über eine Netzwerkverbindung verfügt.
- **WAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielcomputer mindestens WAN-Geschwindigkeit erreicht. WAN-Geschwindigkeit wird als Nicht-RAS-Verbindung definiert, die langsamer als der LAN-Grenzwert ist.
- **LAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielcomputer die LAN-Geschwindigkeitseinstellung überschreitet. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.

Planen von Skripterstellungstasks

Das Fenster **Geplante Tasks** zeigt den Status eines geplanten Tasks an und wird während der Taskausführung und nach Abschluss des Tasks eingeblendet. Der Planungsdienst kann auf zwei Arten mit Geräten kommunizieren:

- Über den Standard Management Agent (muss bereits auf Geräten installiert sein).
- Über ein Systemkonto auf Domänenebene. Auf dem von Ihnen ausgewählten Konto muss das Protokoll als Dienstprivileg installiert sein und Sie müssen Berechtigungsnachweise unter "Configure Services" angegeben haben. Weitere Informationen zum Konfigurieren des Scheduler-Kontos finden Sie unter Konfigurieren des Scheduler-Dienstes.

LANDesk installiert mehrere Standardskripte, die Sie planen können, um routinemäßige Wartungstasks wie die Ausführung von Inventarscans auf ausgewählten Geräten auszuführen. Klicken Sie auf **Skripte** im linken Navigationsfenster und klicken Sie dann auf **Alle anderen Skripte**, um diese Skripte anzuzeigen und zu planen.

So planen Sie einen Task

1. Klicken Sie im linken Navigationsfenster auf **Skripte**.
2. Klicken Sie, um zur Skriptgruppe zu navigieren.
3. Klicken Sie auf ein Skript und klicken Sie auf **Planen**.
4. Geben Sie einen Namen für den Task ein und klicken Sie auf **OK**.
5. Klicken Sie auf der Registerkarte **Benutzerdefinierte Skript-Task** auf **Alle Tasks**, klicken Sie auf den in Schritt 3 benannten Task und klicken Sie auf **Bearbeiten**.
6. Füllen Sie die Seiten des benutzerdefinierten Skript-Tasks aus. Klicken Sie auf die Schaltfläche "Hilfe" auf einer beliebigen Seite oder öffnen Sie die Hilfe zum Task Scheduler an.

Wenn Sie auf **Planen** klicken, wird ein Task erstellt (er verfügt über keine Zielgeräte und keinen Zeitplan). Wenn Sie die Prozedur für den geplanten Task abbrechen, sollten Sie beachten, dass der Task dennoch erstellt wurde und in der Taskliste angezeigt wird.

Verwenden von Standardskripten

Das vorliegende Produkt wird mit zwei Standardskripten geliefert. Diese Skripte können Sie bei der Ausführung häufig anfallender Aufgaben unterstützen. Die Skripte stehen in der Baumansicht

Alle anderen Skripte im Fenster **Skripte** zur Verfügung (linkes Navigationsfenster **| Skripte**) verfügbar.

- **Inventarscanner:** Führt den Inventarscanner auf den ausgewählten Geräten aus. Dieses Skript enthält Beschreibungen zum Erstellen einer Skriptdatei; sehen Sie diese Skriptdatei durch oder drucken Sie sie aus, um weitere Informationen über die korrekte Verwendung von Befehlen und Parametern zu erhalten.
- **Clientdatensätze wiederherstellen:** Führt den Inventarscanner auf ausgewählten Geräten aus, der Scanner berichtet jedoch an den Core, auf dem das Gerät konfiguriert wurde. Wenn Sie die Datenbank zurücksetzen müssen, hilft Ihnen dieser Task, die Geräte in einer Umgebung mit mehreren Cores wieder der richtigen Datenbank zuzuordnen.

Taskplanung

Das Tool **Geplante Tasks** ist Bestandteil der Agentenkonfiguration, Softwareaktualisierungen, Skripte und Geräteerkennung. Die Tasks werden im unteren Fensterausschnitt der entsprechenden Funktionsseiten gefiltert, um nur relevante Tasks anzuzeigen. Wenn Sie beispielsweise das Tool **Geräteerkennung** öffnen, werden Erkennungstasks in der Registerkarte **Erkennungstasks** im unteren Bereich angezeigt. Alle Tasks können nach wie vor über das Tool **Geplante Tasks** angezeigt werden. Hier können Sie festlegen, dass Erkennungskonfigurationen sofort, zu einem späteren Zeitpunkt, wiederholt oder nur einmal ausgeführt werden.

Der linke Fensterausschnitt der Seite **Geplante Tasks** zeigt folgende Taskgruppen:

- **Eigene Tasks:** Tasks, für die Sie einen Zeitplan erstellt haben. Nur Sie selbst und administrative Benutzer können diese Tasks sehen.
- **Alle Tasks:** Sowohl eigene als auch öffentliche Tasks.
- **Globale Tasks:** Tasks, die von Benutzern als "global" gekennzeichnet wurden. Jeder Benutzer, der von dieser Gruppe aus einen Task bearbeitet oder plant, wird Eigentümer dieses Tasks. Der Task verbleibt in der Gruppe "Globale Tasks" und wird auch in der Gruppe "Benutzertasks" für diesen Benutzer angezeigt.
- **Benutzertasks** (nur administrative Benutzer): Von Benutzern erstellte Tasks.

Wenn Sie auf **Eigene Tasks**, **Globale Tasks** oder **Alle Tasks** klicken, werden im rechten Fensterausschnitt folgende Informationen angezeigt:

- **Task:** Die Tasknamen.
- **Starten:** Zeitpunkt, zu dem die Ausführung des Task geplant ist. Klicken Sie auf einen Tasknamen und klicken Sie auf **Bearbeiten**, um die Uhrzeit für den Start zu bearbeiten.
- **Status:** Der Gesamtstatus des Task. Weitere Details finden Sie im rechten Fensterausschnitt in der Spalte "Status". Die Spalte im rechten Fensterausschnitt zeigt den Taskstatus ("In Arbeit", "Alle Vorgänge abgeschlossen", "Kein Vorgang abgeschlossen" oder "Fehlgeschlagen").
- **Verteilungspaket:** Der Name des Pakets, das der Task verteilt. Dieses Feld ist für die Softwareverteilung relevant.
- **Verteilungsmethode:** Die vom Task verwendete Verteilungsmethode. Dieses Feld ist für die Softwareverteilung relevant.
- **Besitzer:** Der Name der Person, die ursprünglich das von diesem Task verwendete Skript erstellt hat.

Wenn Sie auf einen geplanten Task doppelklicken, werden im rechten Fensterausschnitt folgende Informationen angezeigt:

- **Name:** Der Name des Taskstatus.
- **Menge:** Die Geräteanzahl pro Taskstatus.

- **Prozentsatz:** Der Prozentsatz an Geräten in jedem Taskstatus.

Damit Sie die Ausführung geplanter Tasks für ein Gerät planen können, muss auf dem Gerät der entsprechende Agent und das Gerät in der Inventardatenbank registriert sein. Serverkonfigurationen bilden eine Ausnahme. Sie können ein Gerät als Ziel auswählen, auf dem nicht der Standard Management Agent installiert ist. Tasks können auf den Registerkarten "Task" neu geplant (bearbeitet) oder gelöscht werden. Nachdem Sie einen Task geplant haben, können Sie sich auf der Registerkarte "Tasks" über den Taskstatus informieren.

Sie können einen Task bearbeiten, indem Sie den zu bearbeitenden Task auswählen und auf **Bearbeiten** klicken. Der Task wird mit für den Task relevanten Bearbeitungsoptionen geöffnet.

Benutzerdefinierte Taskgruppen

Sie können benutzerdefinierte Gruppe für die Tasktypen **Eigene Tasks**, **Alle Tasks** und **Globale Tasks** erstellen. Mithilfe benutzerdefinierter Gruppen können Sie verwandte Tasks, z. B. das Suchen nach Anfälligkeiten und Ausführen eines Skripts, zu Gruppen zusammenfassen. Gruppen und Untergruppen können bis zu 20 Ebenen enthalten.

So erstellen Sie benutzerdefinierte Taskgruppe

1. Klicken Sie im linken Navigationsfenster auf **Geplante Tasks**.
2. Klicken Sie im linken Bereich auf den Tasktyp, in dem Sie die Gruppe erstellen möchten.
3. Klicken Sie auf **Neue Gruppe** auf der Symbolleiste.
4. Geben Sie einen Namen in das Textfeld **Gruppenname** ein und klicken Sie auf **OK**

Nachdem Sie eine benutzerdefinierte Gruppe erstellt haben, können Sie Tasks oder andere Gruppen in die Gruppe verschieben oder kopieren, indem Sie sie aus einer Liste auswählen und dann auf **Verschieben** in der Symbolleiste klicken.

Die Seite "Zielgeräte"

Verwenden Sie diese Seite, um Geräteziele für den von Ihnen konfigurierten Task hinzuzufügen. Auf dieser Registerkarte können Sie auch die Zielgeräte, Abfragen und Gerätegruppen für den Task anzeigen. Wenn Sie mehrere LANDesk-Verwaltungsprodukte installiert haben, können die in der Konsole eines bestimmten Produkts erstellten Gerätegruppen in allen Konsolen angezeigt werden. Diese Seite wird für Geräteerkennungstasks nicht benötigt.

- **Zielliste hinzufügen:** Fügen Sie die Geräte hinzu, die zuvor aus der Liste **Eigene Geräte** in die Zielliste eingefügt wurden.
- **Abfrage hinzufügen:** Zielt auf die Ergebnisse einer Abfrage ab, die Sie zuvor erstellt hatten.
- **Entfernen:** Entfernt die ausgewählten Ziele.

Hinweis: Obwohl diese Seite als Ziel ausgewählte Gerätegruppen anzeigt, werden Gruppen nur angezeigt, wenn LANDesk Management Suite auf dem Core Server installiert ist. Wenn Sie Server Manager, System Manager oder die Webkonsole in Management Suite ausführen, werden Gerätegruppen nicht als Gruppe als Ziel ausgewählt. Stattdessen werden beim Auswählen einer Gruppe als Ziel die einzelnen Geräte in Gruppe den Zielgerätelisten hinzugefügt und unter **Zielgeräte** anstatt unter **Zielgruppen** angezeigt.

Die Seite "Task planen"

Der Scheduler enthält eine Registerkarte **Geplanter Task – Eigenschaften**, auf der sich diese Optionen befinden.

- **Ungeplant lassen**: (Standard) Bewahrt den Task für künftige Zeitpläne in der Taskliste auf.
- **Jetzt starten**: Führt den Task so bald wie möglich aus. Je nach Einstellung kann es bis zu einer Minute dauern, bevor der Task gestartet wird.
- **Zum geplanten Zeitpunkt starten**: Startet den Task zu der von Ihnen angegebenen Uhrzeit. Wenn Sie auf diese Option klicken, müssen Sie Folgendes eingeben:
    - **Datum**: Das Datum für den Beginn des Tasks. Je nach lokalem Standard ist die Datumsreihenfolge entweder Tag-Monat-Jahr oder Monat-Tag-Jahr.
    - **Uhrzeit**: Die Uhrzeit für den Taskbeginn.
    - **Wiederholen alle**: Wenn der Task wiederholt werden soll, legen Sie durch Klicken auf die entsprechende Schaltfläche fest, ob er **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** ausgeführt werden soll. Wenn Sie **Monat** auswählen und das Datum nicht in allen Monaten existiert (beispielsweise der 31.), wird der Task nur in den Monaten ausgeführt, in denen das Datum existiert.
- **Diese Geräte planen:** Für die erste Ausführung eines Tasks sollten Sie den Standard "Im Wartezustand oder zurzeit aktiv" beibehalten. Für alle weiteren Ausführungen können Sie die Option "Alle", "Fehlgeschlagene Geräte" oder "Geräte, die nicht versucht haben, den Task auszuführen" auswählen. Diese Optionen werden im Folgenden ausführlich beschrieben.
    - **Fehlgeschlagene Geräte:** Wählen Sie diese Option aus, wenn der Task nur auf den Geräten ausgeführt werden soll, auf denen der Task beim ersten Durchlauf nicht ausgeführt werden konnte. Dies schließt Geräte mit dem Status "Erfolgreich" aus. Der Task wird auf Geräten mit anderen Zuständen ausgeführt, beispielsweise "Wartemodus" oder "Aktiv". Ziehen Sie die Verwendung dieser Option in Betracht, wenn Sie den Task auf so vielen Geräten wie möglich ausführen möchten, auf denen die Ausführung misslungen war, der Task jedoch nur einmal pro Gerät erfolgreich ausgeführt werden muss.
    - **Wartezustand oder zurzeit aktiv:** Wählen Sie diese Option aus, wenn Sie den Task auf Geräten ausführen möchten, die sich in der Verarbeitungswarteschlange befinden oder der Verarbeitung zurzeit läuft.
    - **Alle:** Wählen Sie diese Option, wenn Sie den Task, unabhängig vom Zustand, auf allen Geräten ausführen möchten. Ziehen Sie die Verwendung dieser Option in Betracht, wenn Sie einen Task haben (insbesondere einen wiederholt auszuführenden Task), der auf so vielen Geräten wie möglich ausgeführt werden muss.

- **Geräte, die nicht versucht haben, den Task auszuführen:** Wählen Sie diese Option, wenn der Task nur auf Geräten ausgeführt werden soll, die den Task nicht vollständig ausgeführt haben, auf denen die Ausführung aber nicht misslungen war. Dies schließt Geräte aus, deren Zustand "Aus", "Beschäftigt", "Fehlgeschlagen" oder "Abgebrochen" war. Ziehen Sie die Verwendung dieser Option in Betracht, wenn es zahlreiche Zielgeräte gab, auf denen der Task fehlschlug, diese Geräte als Ziele jedoch nicht wichtig sind.

Informationen zur Seite "Benutzerdefinierte Skripte"

- **Zurzeit ausgewähltes benutzerdefiniertes Skript:** Klicken Sie auf das Skript, für das Sie eine Planung durchführen möchten.

Berichte

Informationen zu Berichten

Mit dem Tool für die Berichterstellung in System Manager können Sie eine Vielzahl spezialisierter Berichte erstellen, die wichtige Informationen zu den verwalteten Geräten in Ihrem Netzwerk bereitstellen.

System Manager verwendet einen Inventarscanner, um Geräte (sowie Hard- und Softwaredaten dieser Geräte) zur Core-Datenbank hinzuzufügen. Sie können diese Inventardaten von der Inventaransicht eines Geräts aus einsehen und drucken. Außerdem können Sie die Daten verwenden, um Abfragen zu definieren und Geräte zu Gruppen zusammenzufassen. Das Tool "Berichte" nutzt die gescannten Inventardaten zusätzlich, indem es diese Daten abruft und zu hilfreichen Berichten zusammenfasst.

Sie können die vordefinierten Serviceberichte und Inventarberichte verwenden. Nachdem Sie einen Bericht ausgeführt haben, lässt er sich in der Konsole öffnen.

Wenn Sie Server Manager und Management Suite zusammen installiert haben, enthalten die von Ihnen in Server Manager ausgeführten Berichte nur Server. Wenn Sie eine Abfrage ausführen, werden sowohl Server als auch andere Geräte zurückgegeben, es sei denn, in der Konfiguration der Abfrage wurde die Kategorie "sonstige Geräte" ausgeschlossen.

Wenn Sie den Eindruck haben, dass die Berichterstellung von einem bestimmten Rechner gestoppt wurde, können Sie mithilfe von "restartmon.exe" im Ordner LDCLIENT den Collector und alle Überwachungsanbieter neu starten. Dieses Dienstprogramm ist für Rechner gedacht, auf denen die Berichterstellung installiert wurde, jedoch keine Berichte mehr erstellt werden. Starten Sie mit diesem Dienstprogramm die Collector und Provider neu, ohne das Gerät neu starten zu müssen.

Grundlegendes zu Berichtsgruppen und vordefinierten Berichten

Berichte werden im Fenster **Berichte** (linkes Navigationsfenster **| Berichte**) zu Gruppen zusammengefasst. Administratoren sind berechtigt, den Inhalt aller Berichtgruppen anzuzeigen. System Manager beinhaltet eine spezielle Rolle mit dem Namen "Berichte", die es anderen Benutzern ermöglicht, Berichte anzuzeigen, ohne auf andere Verwaltungsfunktionen zugreifen zu können. Weitere Informationen finden Sie unter Rollenbasierte Administration. Benutzer mit Zugriffsrecht auf Berichte können außerdem auf Geräten in ihrem Bereich Berichte anzeigen und ausführen.

Das Fenster **Berichte** beinhaltet folgende Berichtsgruppen:

- Hardware
- Software

Anzeigen von Berichten

Sie können jeden Bericht vom Fenster **Berichte** aus ausführen.

Klicken Sie vom Fenster **Berichte** aus auf eine Berichtgruppe und klicken Sie dann auf den Bericht, den Sie ausführen möchten. Die Berichtsdaten werden in der **Berichtsansicht** angezeigt.

Informationen zur Berichtsansicht

Berichte bieten Ihnen die Möglichkeit, schnell auf eine grafische Repräsentation des Informationsguthabens auf Ihren Clientcomputern zuzugreifen. Die Berichte werden aus den Daten erstellt, die der Scanner in der Datenbank speichert. Sie können Berichte über Ihren Browser anzeigen oder drucken.

So zeigen Sie einen Bericht an

1. Klicken Sie im linken Navigationsfenster auf **Berichte**. Berichtkategorien werden im rechten Fensterbereich aufgelistet. Klicken Sie auf die Überschrift einer Kategorie, um die Liste mit den Berichten anzuzeigen. Ein Symbol neben dem jeweiligen Bericht gibt den Berichttyp an.

   Ein Bericht, neben dem ein Diagrammsymbol zu sehen ist, wird als Torten- oder Balkendiagramm (zwei- oder dreidimensional) angezeigt. Sie können in einem Diagramm auf einen beliebigen farbigen Balken- oder Tortenabschnitt klicken, um zu einer Zusammenfassung zu gelangen.

   Ein Bericht mit einem Dokumentsymbol wird als Text angezeigt.

2. Klicken Sie auf den Berichtnamen, um den Bericht anzuzeigen.
3. Für die Hardware- oder Softwarescan-Datumsübersicht klicken Sie auf das jeweilige Start- und Enddatum, um den Zeitrahmen festzulegen. Klicken Sie anschließend auf **Ausführen**.

Der Bericht "Festplattenspeicher-Übersicht" enthält ausschließlich Daten für Windows-basierte Geräte.

Um einen Bericht zu drucken, klicken Sie mit der rechten Maustaste auf die Seite und klicken dann auf **Drucken**. Klicken Sie im Dialogfeld "Drucken" auf **Drucken**. Wenn sich ein Bericht über mehrere Seiten erstreckt, klicken Sie mit der rechten Maustaste auf jede Seite, um sie zu drucken.

So verteilen Sie einen Bericht

- Einen Bericht, den Sie per E-Mail weiterleiten möchten, sollten Sie in eine PDF-Datei drucken, die dann der E-Mail als Anhang beigefügt werden kann.

Die Konsole zeigt Berichtdiagramme als Torten- oder Balkendiagramme an. Um den Diagrammtyp festzulegen, klicken Sie auf die Dropdown-Liste im Berichtdiagramm und ändern dann den Diagrammtyp.

Damit die in vielen Berichten enthaltenen interaktiven Balken- und Tortendiagramme angezeigt werden, muss Macromedia Flash Player* 7 installiert sein.

Abfragen

Verwenden von Abfragen

Abfragen sind benutzerdefinierte Suchvorgänge, die in den Core-Datenbanken ausgeführt werden. Dieses Produkt stellt Tools zur Verfügung, mit denen Sie Datenbankabfragen für Geräte in der Core-Datenbank erstellen können. Core-Datenbankabfragen werden in der Ansicht **Abfrage** der Konsole erstellt. System Manager öffentliche Abfragen sind in LANDesk® Management Suite sichtbar und umgekehrt, wenn beide verwendet werden.

In diesem Abschnitt erfahren Sie mehr über:

- Abfragen - Übersicht
- Abfragegruppen
- Erstellen von Datenbankabfragen
- Ausführen von Abfragen
- Importieren und Exportieren von Abfragen

Abfragen - Übersicht

Mithilfe von Abfragen können Sie auf der Basis bestimmter System- oder Benutzerkriterien nach in der Core-Datenbank gespeicherten Geräten suchen und diese entsprechend ordnen. Damit steht Ihnen ein praktisches Hilfsmittel für die Netzwerkverwaltung zur Verfügung.

So können Sie beispielsweise eine Abfrage erstellen und ausführen, die nur Geräte mit einer Taktgeschwindigkeit von weniger als 166 MHz, weniger als 64 MB Arbeitsspeicher oder einer Festplatte mit weniger als 2 GB Speicherkapazität extrahiert. Erstellen Sie eine oder mehrere Abfrageanweisungen für diese Bedingungen und verknüpfen Sie diese Anweisungen mithilfe von logischen Operatoren. Wenn die Abfragen ausgeführt wurden, können Sie die Ergebnisse drucken, auf die entsprechenden Geräte zugreifen und sie verwalten.

Abfragegruppen

Abfragen können in der Ansicht **Eigene Geräte** mit Gruppen verknüpft werden. Diese Gruppen werden als dynamische Gruppen bezeichnet. Der Inhalt einer dynamischen Gruppe ist das Ergebnis der Abfrage, die mit dieser dynamischen Gruppe verknüpft ist. Beispiel: Eine Gruppe, die alle Geräte eines Standorts beinhaltet, kann mit einer Abfrage zu Speicher, Festplattengröße usw. verknüpft werden.

Wenn Sie mehr darüber erfahren möchten, wie Abfragegruppen und Abfragen in der Ansicht **Alle Geräte** angezeigt werden und wie Sie diese Ansicht verwenden können, lesen Sie die Informationen im Abschnitt Gruppieren von Geräten für Aktionen.

Erstellen von Datenbankabfragen

Verwenden Sie das Dialogfeld **Neue Abfrage**, um eine Abfrage durch Auswählen von Attributen, relationalen Operatoren und Attributwerten zu erstellen. Erstellen Sie eine Abfrageanweisung,

indem Sie ein Inventarattribut auswählen und es mit einem akzeptablen Wert verknüpfen. Verknüpfen Sie die Abfrageanweisungen logisch miteinander, um sicherzustellen, dass sie als Gruppe ausgewertet werden, bevor Sie sie mit anderen Anweisungen oder Gruppen verknüpfen.

So erstellen Sie eine Datenbankabfrage

1. Klicken Sie in der Ansicht **Abfragen** der Konsole auf **Neu**.
2. Wählen Sie eine **Komponente** aus der Inventarattributliste aus.
3. Klicken Sie unter **Schritt 1: Suchbedingungen**, klicken Sie auf **Bearbeiten**.
    1. Wählen Sie die Attribute in der Liste aus, die Sie als Suchbedingung festlegen möchten. Um beispielsweise alle Clients zu suchen, die eine bestimmte Software ausführen, wählen Sie Computer.Software.Paket.Name.
    2. Nach dem Auswählen der Attribute wird auf der rechten Seite des Fensters eine Reihe von Feldern angezeigt. Wählen Sie aus diesen Feldern einen Operator und Wert aus, um die Suchbedingung zu vervollständigen. Um beispielsweise alle Clients zu suchen, die Internet Explorer 5.0 ausführen, geben Sie als Attribute "Computer.Software.Paket.Name", als Operator "=" und als Wert "Internet Explorer 5" ein.
    3. Klicken Sie am unteren Fensterrand auf **Hinzufügen**, um das leere Feld mit der Suchbedingung auszufüllen.
    4. Sie können die Abfrage weiter spezifizieren, indem Sie eine weitere Suchbedingung erstellen und sie der ersten Bedingung mit einem Booleschen Operator (AND oder OR) hinzufügen. Über die Schaltflächen können Sie Bedingungen hinzufügen, löschen, ersetzen, gruppieren oder die Gruppierung aufheben.
    5. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.
4. Klicken Sie unter **Schritt 2: Anzuzeigende Attribute**, klicken Sie auf **Bearbeiten**.
    1. Führen Sie einen Drilldown auf dieser Liste durch, um ein Attribut auszuwählen, das in der Abfrageergebnisliste angezeigt werden soll. Wählen Sie dabei Attribute aus, mit denen Sie die in der Abfrage zurückgegebenen Clients identifizieren können. Wenn Sie keine Attribute finden, die Sie anzeigen möchten, können Sie sie im Dialogfeld Benutzerdefinierte Attribute hinzufügen. Diese Attribute müssen jedoch Computern zugewiesen werden, bevor sie im Abfrage-Dialogfeld angezeigt werden.
    2. Klicken Sie nach dem Auswählen eines Attributs auf **Hinzufügen**, um es in das leere Feld unten im Fenster zu verschieben. Wenn Sie die Abfrageergebnisse in der Liste nummerieren möchten, klicken Sie auf **Anzahl aufnehmen**.
    3. Wiederholen Sie den Vorgang, wenn Sie weitere Attribute hinzufügen möchten. Verwenden Sie die Schaltfläche **Entfernen**, um Attribute zu entfernen, und klicken Sie auf **Nach oben/Nach unten** um die Reihenfolge der Attribute zu ändern.
    4. Klicken Sie auf **Ergebnisse als Ziel auswählbar machen**, um die Ergebnisse der Abfrage als Ziel für jede von Ihnen angegebene Aktion auswählbar zu machen.
    5. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.
5. (Optional) Klicken Sie unter **Schritt 3: Ergebnisse nach Attribut sortieren**, klicken Sie auf **Bearbeiten**, um die Reihenfolge Ihrer Abfrageergebnisse anzupassen.
6. Wenn Sie die Abfrage mehrmals ausführen möchten, klicken Sie auf **Abfrage speichern** und geben einen eindeutigen Namen für die Abfrage ein. Wenn Sie die Abfrage ausführen, bevor Sie sie speichern, gehen die Abfrageparameter verloren und müssen wiederhergestellt werden, um dieselbe Abfrage erneut ausführen zu können.
7. Klicken Sie unter **Schritt 4: Abfrage ausführen**, klicken Sie auf **Abfrage ausführen**.

Abfrageanweisungen werden in der gezeigten Reihenfolge ausgeführt.
Wenn keine Gruppierungen vorgenommen werden, werden die in diesem Dialogfeld aufgeführten

Abfrageanweisungen von unten nach oben ausgeführt. Fassen Sie miteinander in Bezug stehende Elemente in Gruppen zusammen, sodass sie als Gruppe ausgewertet werden; andernfalls fallen die Ergebnisse Ihrer Abfrage eventuell anders als erwartet aus.

Ausführen von Abfragen

So führen Sie eine Abfrage aus

1. Klicken Sie im linken Navigationsfenster auf **Abfragen**.
2. Wählen Sie die Abfrage aus und klicken Sie auf **Ausführen**.

   oder

   Wenn Sie die Abfrage vor dem Ausführen ändern möchten, doppelklicken Sie auf die Abfrage, klicken Sie auf **Bearbeiten**, ändern Sie Schritte 1 - 3 und klicken Sie dann auf **Abfrage ausführen**.

   Hinweis: Wenn Sie die Abfrage bearbeitet haben und Ihre Änderungen speichern möchten, klicken Sie auf **Abfrage speichern**, um die Änderungen zu speichern, oder klicken Sie auf **Abfrage speichern unter**, um die geänderte Abfrage unter einem neuen Namen zu speichern. Führen Sie diese Schritte aus, bevor Sie die Abfrage starten. Wenn Sie Ihre Änderungen nicht vor dem Ausführen der Abfrage speichern, werden diese nicht zusammen mit der Abfrage gespeichert.

3. Die Ergebnisse (passenden Geräte) werden im rechten Fensterbereich der Ansicht **Alle Geräte** angezeigt.

Importieren und Exportieren von Abfragen

Sie können über die Import- und Exportfunktionen Abfragen aus einer Core-Datenbank in eine andere übertragen. Exportierte Abfragen werden als .XML-Dateien gespeichert.

So importieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die Abfragegruppe, in welche die Abfrage importiert werden soll.
2. Wählen Sie **Importieren** aus dem Kontextmenü.
3. Navigieren Sie zur Abfrage, die Sie importieren möchten, und wählen Sie sie aus.
4. Klicken Sie auf **Öffnen**, um die Abfrage zur ausgewählten Abfragegruppe in der Ansicht **Alle Geräte** hinzuzufügen.

So exportieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die zu exportierende Abfrage.
2. Wählen Sie **Exportieren** aus dem Kontextmenü.
3. Navigieren Sie zu dem Verzeichnis, in dem Sie die Abfrage (als .XML-Datei) speichern möchten.
4. Geben Sie einen Namen für die Abfrage ein.
5. Klicken Sie auf **Speichern**, um die Abfrage zu exportieren.

Erläuterungen zu benutzerdefinierten Abfragen

Benutzerdefinierte Abfragen sind nützlich, wenn Sie Inventardetails zu Hardware- und Softwareprodukten, die auf Ihren Geräten installiert sind, abrufen möchten. Sie können mithilfe einer benutzerdefinierten Abfrage beispielsweise eine Liste erstellen, in der alle Computer geführt werden, die über ein ähnliches Inventar verfügen. Benutzerdefinierte Abfragen werden auch zum Definieren von Gruppen und Bereichen verwendet.

Die Seite **Benutzerdefinierte Abfragen** (im linken Navigationsfenster auf **Abfragen** klicken) enthält eine Liste mit Abfragen, die Sie gespeichert haben. Um eine gespeicherte Abfrage auszuführen, wählen Sie die Abfrage und dann **Ausführen**.

Wenn sich das Abfrageergebnis über mehrere Seiten erstreckt, können Sie mit den Pfeilen am oberen Seitenrand zwischen den Seiten hin- und herblättern. Geben Sie an, wie viele Elemente pro Seite angezeigt werden sollen, und klicken Sie auf **Festlegen**.

Erstellen benutzerdefinierter Abfragen

Benutzerdefinierte Abfragen sind nützlich, wenn Sie Inventardetails zu Hardware- und Softwareprodukten, die auf Ihren Geräten installiert sind, abrufen möchten. Verwenden Sie eine benutzerdefinierte Abfrage dazu, Geräte, die über ein ähnliches Inventar verfügen, in einer Liste zusammenzufassen. Wenn Sie beispielsweise Geräte auf einen Prozessor mit 750 MHz aufrüsten möchten, können Sie alle Geräte mit einer Prozessorgeschwindigkeit unter 750 MHz aus der Datenbank extrahieren. Benutzerdefinierte Abfragen werden auch zum Definieren von Gruppen und Bereichen verwendet.

Sie können alle Inventarelemente ("Attribute" genannt), die der Inventarscanner in der Datenbank speichert, sowie alle benutzerdefinierten Attribute abfragen.

Verwalten von Abfragen

Verwalten Sie Abfragen in der Ansicht **Abfragen**. Verwenden Sie diese Ansicht zum Erstellen, Bearbeiten oder Löschen von Abfragen:

- Um eine vorhandene Abfrage auszuführen, wählen Sie sie aus und klicken auf **Ausführen**.
- Um eine neue Abfrage zu erstellen, klicken Sie auf **Neu**. Sobald Sie die Abfrage erstellt und gespeichert haben, wird der Name in der Liste auf dieser Seite angezeigt.
- Zum Bearbeiten einer Abfrage in der Liste doppelklicken Sie auf die Abfrage. Die Seite **Abfrage bearbeiten** wird angezeigt. Sie enthält Abfrageparameter, die von Ihnen bearbeitet werden können.
- Zum Bearbeiten der letzten Abfrage klicken Sie auf **Aktuelle Abfrage bearbeiten**.
- Um eine Abfrage zu entfernen, wählen Sie die Abfrage aus und klicken auf **Löschen**.

Zum Erstellen einer Abfrage sind vier Schritte erforderlich:

1. **Eine Suchbedingung erstellen:** Geben Sie eine Reihe von Inventarattributen an, die die Grundlage der Abfrage bilden.
2. **Attribute zum Anzeigen auswählen:** Verfeinern oder "filtern" Sie die Abfrage so, dass die Ergebnisse die für Sie nützlichsten Attribute anzeigen, wie z. B. IP-Adressen oder Gerätenamen.
3. **Ergebnisse nach Attribut sortieren (optional):** Geben Sie an, wie die Abfrageergebnisse sortiert werden sollen. (Dies trifft nur zu, wenn Sie in Schritt 2 mehr als einen Attributtyp zur Anzeige in den Abfrageergebnissen ausgewählt haben.)
4. **Abfrage ausführen:** Führen Sie die soeben erstellte Abfrage aus. Sie können sie auch zur späteren Verwendung speichern oder alle Abfragedaten löschen und eine neue Abfrage erstellen.

Schritt 1: Erstellen einer Suchbedingung (erforderlich)

Eine Suchbedingung besteht aus einer Reihe von Inventarattributen und verknüpften Werten, die von Ihnen abgefragt werden. Als Grundlage für eine Abfrage können Sie eine einzelne Suchbedingung verwenden oder mehrere Suchbedingungen zu einer Gruppe zusammenstellen.

Die folgenden Schritte führen Sie auf der Seite **Abfrage bearbeiten** aus. Klicken Sie von der Anzeige **Abfrage ausführen** aus auf **Neu**, oder wählen Sie eine vorhandene Abfrage aus und klicken Sie auf **Bearbeiten**.

So erstellen Sie eine Suchbedingung

1. Klicken Sie unter **Schritt 1** auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
2. Wählen Sie die Attribute in der Liste aus, die Sie als Suchbedingung festlegen möchten. Um beispielsweise alle Clients zu suchen, die eine bestimmte Software ausführen, wählen Sie Computer.Software.Paket.Name.
3. Nach dem Auswählen der Attribute wird auf der rechten Seite des Fensters eine Reihe von Feldern angezeigt. Wählen Sie aus diesen Feldern einen Operator und Wert aus, um die Suchbedingung zu vervollständigen. Um beispielsweise alle Clients zu suchen, die Internet Explorer 5.0 ausführen, geben Sie als Attribute "Computer.Software.Paket.Name", als Operator "=" und als Wert "Internet Explorer 5" ein.
4. Klicken Sie am unteren Fensterrand auf **Hinzufügen**, um das leere Feld mit der Suchbedingung auszufüllen.
5. Sie können die Abfrage weiter spezifizieren, indem Sie eine weitere Suchbedingung erstellen und sie der ersten Bedingung mit einem Booleschen Operator (AND oder OR) hinzufügen. Über die Schaltflächen können Sie Bedingungen hinzufügen, löschen, ersetzen, gruppieren oder die Gruppierung aufheben.
6. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

Bevor Sie eine Abfrage zum Zustand eines Servers (Computer.Health.State) ausführen und speichern, sollten Sie berücksichtigen, dass der Zustand des Servers in der Datenbank durch eine Nummer repräsentiert wird. Verwenden Sie die Tabelle weiter unten, um Suchbedingungen zu erstellen. Um z. B. eine Suchbedingung für Rechner mit dem Zustand "Unbekannt" zu erstelllen, verwenden Sie den Operator "NOT EXIST".

Zustand	Operator

Zustand	Operator
Unbekannt	NOT EXIST
Normal	2
Warnung	3
Kritisch	4

Schritt 2: Auswählen der anzuzeigenden Attribute (erforderlich)

In Schritt 2 wählen Sie Attribute aus, die besonders nützlich sind, um die in den Abfrageergebnissen zurückgegebenen Computer zu identifizieren. Wenn Sie anhand der Ergebnisse beispielsweise jeden Computer, der den in Schritt 1 angegebenen Suchbedingung entspricht, physikalisch orten möchten, geben Sie Attribute wie den Anzeigenamen des Computers (Computer.Anzeigename) oder die IP-Adresse (Computer.Netzwerk.TCPIP.Adresse) an.

Die folgenden Schritte führen Sie auf der Seite **Abfrage bearbeiten** aus.

So wählen Sie Attribute zum Anzeigen aus

1. Klicken Sie unter **Schritt 2** auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
2. Führen Sie einen Drilldown auf dieser Liste durch, um ein Attribut auszuwählen, das in der Abfrageergebnisliste angezeigt werden soll. Wählen Sie dabei Attribute aus, mit denen Sie die in der Abfrage zurückgegebenen Clients identifizieren können. Wenn Sie keine Attribute finden, die Sie anzeigen möchten, können Sie sie im Dialogfeld Benutzerdefinierte Attribute hinzufügen. Diese Attribute müssen jedoch Computern zugewiesen werden, bevor sie im Abfrage-Dialogfeld angezeigt werden.

   Hinweis: Wenn Sie eine Oracle-Datenbank verwenden, wählen Sie mindestens ein Attribut aus, das direkt durch den Inventarscanner definiert ist (z. B. Computer.Anzeigename, Computer.Gerätename, Computer.Gerätekennung, Computer.Anmeldename usw.).

3. Klicken Sie nach dem Auswählen eines Attributs auf **>>**, um es in das leere Feld auf der rechten Seite des Fensters zu verschieben. Wenn Sie die Abfrageergebnisse in der Liste nummerieren möchten, klicken Sie auf **Anzahl aufnehmen**.
4. Wiederholen Sie den Vorgang, wenn Sie weitere Attribute hinzufügen möchten. Verwenden Sie die Pfeiltasten, um Attribute hinzuzufügen oder zu entfernen. Klicken Sie auf **Nach oben/Nach unten**, um die Reihenfolge der Attribute zu ändern.
5. Klicken Sie auf **Ergebnisse als Ziel auswählbar machen**, um die Ergebnisse der Abfrage als Ziel für jede von Ihnen angegebene Aktion auswählbar zu machen.

6. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

Sie können auch Spaltenüberschriften zur Liste mit den Abfrageergebnissen hinzufügen.

So ändern Sie Spaltenüberschriften (optional)

1. Klicken Sie unter **Schritt 2** auf **Bearbeiten**.
2. Klicken Sie im unteren Feld auf eine Spaltenüberschrift und klicken Sie dann auf **Bearbeiten**. Bearbeiten Sie die Überschrift und drücken Sie die **Eingabetaste**. Wiederholen Sie diesen Schritt nach Bedarf.
3. Klicken Sie auf **OK**.

Speichern Sie nun gegebenenfalls die Abfrage. Der nächste Schritt im Abfrageerstellungsprozess ist optional und gilt nur für Abfrageergebnisse, die zwei oder mehr Spalten enthalten. Klicken Sie zum Speichern der Abfrage auf **Abfrage speichern** oben auf der Seite. Es wird ein Fenster angezeigt und Sie werden zur Eingabe eines Namens für diese Abfrage aufgefordert. Geben Sie einen Namen ein und klicken Sie anschließend in der rechten oberen Ecke des Fensters auf **Speichern**.

Schritt 3: Sortieren der Ergebnisse nach Attribut (optional)

Diese Prozedur muss nur ausgeführt werden, wenn Sie in Schritt 2 mehr als ein Attribut oder eine Spaltenüberschrift definiert haben und die Ergebnisse alphabetisch oder nummerisch innerhalb einer Spalte sortieren möchten.

Angenommen, Sie haben zwei verschiedene Attribute angegeben, die in den Abfrageergebnissen angezeigt werden sollen: die IP-Adresse und den Prozessortyp des zurückgegebenen Computers. In Schritt 3 könnten Sie die Ergebnisse alphabetisch nach Prozessortyp sortieren.

Wenn Sie diesen Schritt überspringen, wird die Abfrage automatisch nach dem ersten, in Schritt 2 gewählten Attribut sortiert.

So sortieren Sie die Ergebnisse nach Attribut

1. Klicken Sie unter **Schritt 3** auf **Bearbeiten**. Es wird ein Fenster geöffnet, in dem die von Ihnen in **Schritt 2** ausgewählten Attribute angezeigt werden.
2. Wählen Sie das Attribut, nach dem sortiert werden soll, und klicken Sie anschließend auf **>>**, um es in das leere Textfeld zu verschieben.
3. Klicken Sie auf **OK**.

Schritt 4: Ausführen der Abfrage

Nachdem Sie Ihre Abfrage erstellt haben, können Sie sie ausführen, speichern oder löschen (falls Sie noch einmal von vorne beginnen möchten).

Um die Abfrage für eine zukünftige Verwendung zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern**. Die Abfrage wird nun auf der Seite **Benutzerdefinierte Abfragen** aufgelistet. Wenn es sich bei Ihrer Abfrage um eine geänderte Version einer anderen Abfrage

handelt, klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern unter**, um sie umzubenennen.

Standardmäßig sind gespeicherte Abfragen nur für den Benutzer sichtbar, der sie gespeichert hat. Wenn Sie vor dem Speichern das Kontrollkästchen **Öffentliche Abfrage** aktivieren, ist die Abfrage für alle Benutzer sichtbar. Nur Administratoren, die befugt sind, öffentliche Abfragen zu verwalten, können eine Abfrage öffentlich machen.

Wenn Sie mehrere Produkte der Produktreihe installiert haben, werden Abfragen von den Produkten gemeinsam genutzt. Wenn Sie eine Abfrage in der Konsole eines bestimmten Produkts speichern, ist diese Abfrage auch auf anderen Produktkonsolen zu sehen.

Zum Anzeigen der Ergebnisse dieser Abfrage klicken Sie auf die Symbolleistenschaltfläche **Ausführen**.

Um die Abfrageparameter auf der Seite **Anbfrage bearbeiten** zu beseitigen, klicken Sie auf die Symbolleistenschaltfläche **Löschen** . Wurde die Abfrage bereits gespeichert, wird sie auf dieser Seite entfernt, bleibt aber in der Liste **Benutzerdefinierte Abfragen** gespeichert.

Anzeigen von Abfrageergebnissen

Abfrageergebnisse stimmen mit den Suchkriterien überein, die Sie beim Definieren der Abfrage angegeben haben. Wenn die Ergebnisse nicht Ihren Erwartungen entsprechen, gehen Sie zurück zur Seite **Abfrage bearbeiten** und bearbeiten Sie die Informationen.

Um durch einen Drilldown weitere Informationen zu einem Gerät zu erhalten, das in der Liste mit den Abfrageergebnissen aufgeführt ist, müssen Sie auf die Abfragedaten doppelklicken oder mit der rechten Maustaste klicken und in dem anschließend eingeblendeten Menü auf **Computer anzeigen** klicken.

Auf der Seite **Abfrageergebnisse** können Sie in der Symbolleiste auf die Schaltfläche **Speichern unter CSV** klicken, um die Ergebnisse in einem Format zu exportieren, das mit Tabellenkalkulationsprogrammen oder anderen Anwendungen kompatibel ist.

Um die Abfrageergebnisse zu drucken, klicken Sie auf **Seitenansicht** auf der Seite "Abfrageergebnisse".

Anzeigen von Ergebnissen einer Drilldown-Abfrage

Abfrageergebnisse stimmen mit den Suchkriterien überein, die Sie beim Definieren der Abfrage angegeben haben. Wenn die Ergebnisse nicht Ihren Erwartungen entsprechen, gehen Sie zurück zur Seite **Abfrage bearbeiten** und bearbeiten Sie die Informationen.

Um durch einen Drilldown weitere Informationen zu einem Gerät zu erhalten, das in der Liste mit den Abfrageergebnissen aufgeführt ist, müssen Sie auf die Abfragedaten doppelklicken oder mit der rechten Maustaste klicken und in dem anschließend eingeblendeten Menü auf **Computer anzeigen** klicken.

Exportieren von Abfrageergebnissen in CSV-Dateien

Um die Ergebnisdaten Ihrer Abfrage in einem Tabellenkalkulationsprogramm anzuzeigen, exportieren Sie die Daten als Datei mit durch Kommas getrennten Werten (CSV-Datei). Klicken Sie auf der Seite **Abfrageergebnisse** auf das Symbolleistensymbol **Speichern unter CSV**, um Ihre Daten als CSV-Datei zu speichern. Anschließend können Sie die CSV-Datei in ein Tabellenkalkulationsprogramm wie Microsoft Excel* importieren und dort bearbeiten.

Ändern der Spaltenüberschriften für Abfragen

1. Öffnen Sie eine vorhandene Abfrage oder erstellen Sie eine neue Abfrage.
2. Klicken Sie im unteren Feld auf eine Spaltenüberschrift und klicken Sie dann auf **Bearbeiten**. Bearbeiten Sie die Überschrift und drücken Sie die **Eingabetaste**. Wiederholen Sie diesen Schritt nach Bedarf.
3. Klicken Sie auf **OK**.

Exportieren und Importieren von Abfragen

Sie können jede von Ihnen erstellte Abfrage exportieren oder importieren. Alle Abfragen werden als XML-Dateien exportiert. Wenn Sie eine Abfrage mit demselben Dateinamen mehr als einmal exportieren, wird die vorhandene Datei überschrieben. Um dies zu verhindern, können Sie die Datei nach dem Exportieren an einen anderen Speicherort kopieren.

Die Funktionen zum Exportieren und Importieren sind in zwei Szenarien nützlich:

- Wenn Sie Ihre Datenbank erneut installieren müssen, verwenden Sie die Export- und Importfunktionen, um Ihre vorhandenen Abfragen für die Verwendung in einer neuen Datenbank zu speichern.

  Sie können die Abfragen beispielsweise exportieren und anschließend in ein Verzeichnis verschieben, das von einer Datenbankneuinstallation nicht betroffen ist. Nachdem Sie die Datenbank neu installiert haben, können Sie die Abfragen wieder in das Abfrageverzeichnis auf Ihrem Webserver verschieben und anschließend in die neue Datenbank importieren.

- Sie können die Export-/Importfunktionen zum Kopieren von Abfragen in andere Datenbanken verwenden.

  Sie können beispielsweise eine Abfrage in ein Abfrageverzeichnis auf Ihrem Webserver exportieren und dann per E-Mail oder FTP an eine andere Person weiterleiten. Dieser Benutzer kann die Abfragen dann in ein Abfrageverzeichnis auf einem anderen Webserver speichern und anschließend in eine Datenbank importieren. Sie können auch ein Laufwerk zuweisen und die Abfragen direkt in das Abfrageverzeichnis eines anderen Webservers kopieren.

So exportieren Sie eine Abfrage

Führen Sie die folgenden Schritte aus, während Sie mit einer Datenbank verbunden sind, in der sich die zu exportierende Abfrage befindet.

1. Klicken Sie im linken Navigationsfenster auf **Abfragen**.
2. Klicken Sie auf der Seite **Benutzerdefinierte Abfragen** auf den Namen der zu exportierenden Abfrage. Klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Abfrage bearbeiten** in der Symbolleiste auf die Schaltfläche **Exportieren**, um die Abfrage nach einem Datenträger zu exportieren.
4. Klicken Sie auf der Seite **Abfrage exportiert** mit der rechten Maustaste auf die Abfrage, um sie als XML-Datei in einem ausgewählten Verzeichnis zu speichern. Aus der Abfrage wird jetzt eine XML-Datei.

Hinweis: Wenn Sie eine Abfrage mit demselben Dateinamen mehr als einmal exportieren, wird die vorhandene Datei überschrieben. Um dies zu verhindern, können Sie die Datei nach dem Exportieren an einen anderen Speicherort kopieren.

Wenn Sie die Abfrage wieder in eine Datenbank importieren möchten, verschieben Sie sie in das Abfrageverzeichnis, das vom Webserver erkannt wird (standardmäßig c:\inetpub\wwwroot\LANDesk\LDSM\queries).

So importieren Sie eine Abfrage

Führen Sie die folgenden Schritte aus, während Sie mit der Datenbank verbunden sind, in die Sie eine Abfrage importieren möchten.

1. Klicken Sie im linken Navigationsfenster auf **Abfragen**.
2. Klicken Sie auf der Seite **Benutzerdefinierte Abfragen** auf **Neu**.
3. Klicken Sie auf der Seite **Abfrage bearbeiten** auf die Symbolleistenschaltfläche **Importieren**.
4. Wählen Sie die Abfrage aus, die Sie importieren möchten. Wenn Sie die Parameter dieser Abfrage vor dem Importieren überprüfen möchten, klicken Sie auf **Ansicht**.
5. Klicken Sie auf **Importieren**, um die Abfrage in die Seite **Abfrage bearbeiten** zu laden.
6. Sobald die Abfrage geladen ist, scrollen Sie nach unten und klicken auf **Abfrage speichern**, um die Abfrage in dieser Datenbank zu speichern.

Inventarverwaltung

Sie können das Inventarscanner-Dienstprogramm verwenden, um Geräte zur Core-Datenbank hinzuzufügen und Informationen zur Hardware und Software des Geräts zu sammeln. Sie können Inventardaten anzeigen, drucken und exportieren. Sie können mit dem Inventarscanner zudem Abfragen definieren, Server zu Gruppen zusammenfassen und benutzerdefinierte Berichte generieren.

In diesem Abschnitt erfahren Sie mehr über:

Übersicht über das Inventarscannen

Wenn Sie ein Gerät mit der Geräte-Setup-Funktion konfigurieren, gehört der Inventarscanner zu den auf dem Gerät installierten Komponenten. Beim Erstellen einer Clientkonfiguration können Sie angeben, wann der Inventarscanner auf dem Gerät ausgeführt werden soll.

Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Der Name der Scanner-Programmdatei lautet für Windows LDISCAN32.EXE und für Linux LDISCAN. Der Inventarscanner erfasst Hard- und Softwaredaten und fügt sie in die Core-Datenbank ein. Danach wird der Hardwarescan bei jedem Gerätestart ausgeführt. Im Gegensatz dazu läuft der Softwarescan nur in einem von Ihnen festgelegten Intervall. Um die Einstellungen für den Softwarescan zu konfigurieren, klicken Sie auf dem Core Server auf **Start | Programme | LANDesk | LANDesk Dienste konfigurieren**.

Weitere Informationen zum Konfigurieren des Inventardienstes finden Sie unter Konfigurieren des Inventardienstes in Anhang C.

Nach dem ersten Scan kann der Inventarscanner von der Konsole aus als geplanter Task ausgeführt werden. Um einen Inventarscan auf Remote-Servern planen zu können, muss auf diesen Geräten der Standard Management Agent laufen.

Hinweis: Ein Gerät, das über die Erkennungsfunktion zur Core-Datenbank hinzugefügt wurde, hat seine Inventardaten noch nicht in die Core-Datenbank gescannt. Sie müssen einen Inventarscan auf jedem Gerät ausführen, damit die gesamten Inventardaten für dieses Gerät angezeigt werden.

Sie können Inventardaten anzeigen lassen und wie folgt verwenden:

- Die Spalten in der Liste **Alle Geräte** anpassen, um bestimmte Inventarattribute anzuzeigen.
- Die Core-Datenbank nach Servern mit bestimmten Inventarattributen durchsuchen
- Fassen Sie Geräte in Gruppen zusammen, um Verwaltungsaufgaben zu beschleunigen
- Spezielle Berichte basierend auf Inventarattributen generieren

- Hardware- und Softwareänderungen auf Geräten verfolgen und Alarme oder Protokolleinträge generieren, wenn solche Änderungen stattfinden.

In den folgenden Abschnitten erfahren Sie mehr über die Funktionsweise des Inventarscanners.

Abstandsscannen (Delta-Scan)

Nach dem ersten vollständigen Scan auf einem Gerät erfasst der Inventarscanner bei nachfolgenden Scans nur Delta-Änderungen und sendet diese an die Core-Datenbank. Verwenden Sie die Scanneroption /RSS zum Abrufen von Softwareinformationen aus der Windows-Registrierung.

Erzwingen eines vollständigen Scans

Wenn Sie einen vollständigen Scan der Hardware- und Softwaredaten des Geräts erzwingen möchten, können Sie die vorhandene Delta-Scan-Datei löschen und die entsprechende Einstellung im Applet **LANDesk Software Services konfigurieren** ändern.

1. Löschen Sie die Datei **invdelta.dat** aus dem Server. Eine Kopie des letzten Inventarscans ist lokal als verborgene Datei mit dem Namen "invdelta.dat" im Root-Verzeichnis des Laufwerks gespeichert. (Die Umgebungsvariable LDMS_LOCAL_DIR legt den Pfad dieser Datei fest.)
2. Fügen Sie die Option **/sync** in die Befehlszeile des Inventarscanners ein. Um die Befehlszeile zu bearbeiten, klicken Sie auf **Start | Alle Programme | LANDesk Management**, klicken mit der rechten Maustaste auf das Verknüpfungssymbol **Inventarscan**, wählen **Eigenschaften | Verknüpfung** aus und bearbeiten dann den **Zielpfad**.
3. Klicken Sie auf dem Core Server auf **Start | Alle Programme | LANDesk | LANDesk - Dienste konfigurieren**.
4. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
5. Klicken Sie auf die Einstellung **Do Delta**. Geben Sie in das **Wert**-Feld **0** ein.
6. Klicken Sie zweimal auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Scankomprimierung

Inventarscans mit dem Windows-Inventarscanner (LDISCAN32.EXE) werden standardmäßig komprimiert. Der Scanner komprimiert vollständige und Abstandsscans in einem Komprimierungsverhältnis von ca. 8:1. Scans werden zunächst vollständig im Speicher erstellt, dann komprimiert und mithilfe eines größeren Pakets an den Core Server gesendet. Die Scankomprimierung reduziert die Anzahl der erforderlichen Pakete und die Bandbreitennutzung.

Scanverschlüsselung

Inventarscans sind verschlüsselt (nur TCP/IP-Scans). Sie können die Inventarscan-Verschlüsselung deaktivieren, indem Sie die entsprechende Einstellung im LANDesk Configure Services-Applet ändern.

1. Klicken Sie auf dem Core Server auf **Start | Alle Programme | LANDesk | LANDesk - Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
3. Klicken Sie auf die Einstellung **Verschlüsselung deaktivieren**. Geben Sie in das **Wert**-Feld **1** ein.
4. Klicken Sie auf **Festlegen** und klicken Sie dann auf **OK**.
5. Klicken Sie zweimal auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Anzeigen von Inventardaten

Sobald ein Gerät vom Inventarscanner geprüft wurde, können Sie dessen Systeminformationen in der Konsole anzeigen.

Die Inventardaten des Geräts werden in der Core-Datenbank gespeichert. Sie umfassen Hardware-, Gerätetreiber-, Software-, Speicher- und Umgebungsinformationen. Die Inventarinformationen sind beim Verwalten und Konfigurieren von Geräten hilfreich. Außerdem können Sie damit schnell Systemprobleme erkennen.

Inventardaten können folgendermaßen angezeigt werden:

- Inventarzusammenfassung
- Vollständiges Inventar
- Anzeigen von Attributeigenschaften
- Systeminformationen

Darüber hinaus können Inventardaten auch in von Ihnen generierten Berichten angezeigt werden. Weitere Informationen finden Sie unter Übersicht über Berichte.

Anzeigen der Inventarübersicht auf der Serverinformationskonsole

Die Inventarübersicht auf der Seite **Übersicht** in der Serverinformationskonsole bietet einen schnellen Überblick über die Betriebssystemkonfiguration sowie Systeminformationen des Geräts.

Hinweis: Wenn Sie ein Gerät mithilfe des Erkennungstool in die Core-Datenbank eingefügt haben, sind seine Inventardaten noch nicht in die Core-Datenbank gescannt. Sie müssen einen Inventarscan auf dem Server ausführen, damit die Inventarübersicht erfolgreich erstellt werden kann.

So zeigen Sie eine Inventarzusammenfassung an

1. Doppelklicken Sie in der Konsolenansicht **Alle Geräte** auf ein Gerät.
2. Klicken Sie im linken Navigationsfenster auf **Systeminformationen** und klicken Sie auf **Systemübersicht**.

Datenübersicht - Windows 2000 / 2003-Server

Diese Informationen werden eingeblendet, wenn Sie die Inventarübersicht für einen Windows 2000/3000-Server anzeigen.

- **Zustand:** Der aktuelle Zustand des Servers.
- **Typ:** Der Servertyp, beispielsweise Anwendung, Datei, E-Mail usw.
- **Hersteller:** Der Hersteller des Servers.
- **Modell:** Das Servermodell.
- **BIOS-Version:** Die ROM BIOS-Version.
- **Betriebssystem:** Windows- oder Linux-Betriebssystem, das auf dem Server ausgeführt wird: 2000, 2003 oder Red Hat.
- **Betriebssystemversion:** Versionsnummer des Windows 2000/2003- oder Linux-Betriebssystems, das auf dem Server ausgeführt wird.
- **CPU:** Auf dem Server ausgeführte(r) Prozessor bzw. Prozessoren.
- **Anfälligkeitsscanner:** Die Version des installierten Agenten.
- **Inventarscanner:** Die Version des installierten Agenten.
- **Überwachung:** Die Version des installierten Überwachungsscanners.
- **Letzter Neustart:** Zeitpunkt, zu dem der Server das letzte Mal neu gestartet wurde.
- **CPU-Nutzung:** Prozentsatz des Prozessors, der gegenwürtig benutzt wird.
- **Physikalischer Speicher verwendet:** Auf dem Server verfügbarer RAM.
- **Virtueller Speicher verwendet:** Dem Server auf dem Gerät zur Verfügung stehender Speicher, einschließlich RAM und Speicher der Auslagerungsdatei.
- **Laufwerksspeicherplatz belegt:** Zurzeit belegter Speicherplatz (in %). Wenn Sie mehrere Festplattenlaufwerke besitzen, wird jedes Laufwerk einzeln aufgeführt.

IPMI-kompatible Server zeigen zusätzliche IPMI-spezifische Daten an. Für Linux-Server werden ähnliche Informationen in der **Übersicht** angezeigt.

Anzeigen eines vollständigen Inventars

Ein vollständiges Inventar umfasst eine komplette und ausführliche Aufstellung der Hardware- und Softwarekomponenten eines Geräts. Die Aufstellung enthält Objekte und Objektattribute.

So zeigen Sie ein vollständiges Inventar an

1. Klicken Sie in der Ansicht **Alle Geräte** der Konsole auf ein Gerät.
2. Klicken Sie auf der Registerkarte **Eigenschaften** auf **Inventar anzeigen**.

Anzeigen von Attributeigenschaften

In der Inventarliste können Sie Attributeigenschaften für die Inventarobjekte eines Geräts anzeigen. Attributeigenschaften geben Aufschluss über die Eigenschaften und Werte eines Inventarobjekts. Sie können auch neue, angepasste Attribute erstellen und benutzerdefinierte Attribute bearbeiten.

Um die Eigenschaften eines Attributs anzuzeigen, klicken Sie im linken Fensterbereich auf das betreffende Attribut.

Sie können diese Informationen in Internet Explorer drucken, indem Sie mit der rechten Maustaste in den Frame und dann auf **Drucken** klicken. Um in Mozilla zu drucken, klicken Sie mit der rechten Maustaste in den Frame, klicken auf **This Frame | Save Frame As**, klicken auf **Save**, öffnen dann die Datei in einer Anwendung und klicken auf **Print**.

Systeminformationen

Von der Serverinformationskonsole aus können Sie die Systeminformationen des Geräts anzeigen und ändern. Informationen in den Kategorien **Hardware**, **Software**, **Protokolle** und **Weitere** sind entweder gespeicherte Daten oder Echtzeitdaten. Sobald Sie auf eine Informationsverknüpfung klicken, können Sie detaillierte Informationen zu der ausgewählten Komponente anzeigen und ggf. Grenzwerte definieren und Informationen eingeben.

1. Doppelklicken Sie in der Konsolenansicht **Alle Geräte** auf ein Gerät.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Systeminformationen**.
3. Erweitern Sie die Gruppe und klicken Sie auf die Informationsverknüpfung, die Sie anzeigen möchten.

Anpassen von Inventaroptionen

Mit dem Programm "Dienste konfigurieren", das zur Webkonsole gehört, können Inventaroptionen angepasst werden. Die Standardeinstellungen sind für die meisten Optionen die richtige Wahl, wenn Sie sie jedoch ändern müssen, können Sie dies tun, indem Sie dieses Dienstprogramm ausführen. Um das Applet "Dienste konfigurieren" auf dem Core Server zu starten, klicken Sie auf **Start | Programme | LANDesk | LANDesk Dienste konfigurieren**. (Der Dateiname dieses Programms lautet "svccfg.exe".)

Verwenden Sie "Dienste starten" zum Konfigurieren der folgenden Einstellungen:

- Datenbankname, Benutzername und Kennwort
- Softwarescan-Intervall für Geräte, Wartung, Speicherzeitraum für Inventarscans (in Tagen) und Länge des Protokolls der Clientanmeldung
- Handhabung doppelt vorhandener Geräte-IDs
- Scheduler-Konfiguration, einschließlich des Intervalls zwischen geplanten Aufträgen und Abfrageevaluierungen
- Benutzerdefinierte Auftragskonfiguration, einschließlich Zeitüberschreitungswert für die Fernausführung

Klicken Sie auf **Hilfe** auf der jeweiligen Registerkarte im Dienstprogramm "Dienste konfigurieren", um weitere Informationen zu erhalten.

Bearbeiten der LDAPPL3.TEMPLATE-Datei

Speziell auf die Scanner-Inventarparameter bezogene Informationen sind in der Datei LDAPPL3.TEMPLATE enthalten. Diese Vorlagendatei identifiziert in Zusammenarbeit mit der Datei LDAPPL3.INI das Softwareinventar eines Geräts. Die Datei wird auf verwalteten Windows-Geräten als Teil der Agentenkonfiguration abgelegt. Ihre Parameter werden auf der Registerkarte "Inventar" der Agentenkonfiguration festgelegt.

Auf Linux-Geräten beinhaltet eine ähnliche Konfigurationsdatei (/etc/ldappl.conf) Informationen zu den Parametern des Scanners. Sie können diese Datei bearbeiten, um die Arbeitsweise des Scanners zu ändern. Die Datei enthält Anweisungen dazu, wie die Funktionsweise des Linux-Scanners geändert werden kann.

Sie können den Abschnitt [LANDesk-Inventar] der Vorlagendatei bearbeiten, um die Parameter zu konfigurieren, die festlegen, wie der Scanner das Softwareinventar erkennt. Standardmäßig ist LDAPPL3.TEMPLATE in der LDLogon-Freigabe auf dem Core Server gespeichert.

Verwenden Sie diese Tabelle als Richtlinie beim Bearbeiten des Abschnitts [LANDesk-Inventar] in einem Texteditor.

Option	Beschreibung
Modus	Bestimmt, wie der Scanner auf den Geräten nach Software scannt. Standard ist "Aufgelistete". Es gibt folgende Einstellungen: • **Aufgelistete:** Zeichnet die Dateien auf, die in LDAPPL3 aufgeführt sind. • **Nicht aufgelistete:** Zeichnet Name und Datum aller Dateien auf, deren Erweiterungen in der Zeile "ScanExtensions" aufgeführt, jedoch nicht in LDAPPL3 definiert sind. Mit dieser Methode lässt sich nicht autorisierte Software auf dem Netzwerk finden. • **Alle:** Findet aufgelistete und nicht aufgelistete Dateien.
Duplikat	Zeichnet Mehrfachinstanzen von Dateien auf. Setzen Sie den Wert auf OFF, um nur die erste Instanz aufzuzeichnen, oder auf ON, um alle gefundenen Instanzen aufzuzeichnen. Standard ist ON.
ScanExtensions	Legt die Dateierweiterungen fest (.EXE, .COM, .CFG usw.), nach denen gescannt wird. Trennen Sie die Erweiterungen durch ein Leerzeichen voneinander. Standardmäßig werden nur .EXEs gescannt.
Version	Die Versionsnummer der Datei LDAPPL3 .
Revision	Die Revisionsnummer der Datei LDAPPL3, die für zukünftige Kompatibilität sorgt.
CfgFiles 1-4	Zeichnet Datum, Uhrzeit, Dateigröße und Inhalt der entsprechenden Dateien auf. Lassen Sie den Laufwerksbuchstaben (z.B. c:) weg, wenn Sie alle lokalen Laufwerke durchsuchen möchten. Sie können mehr als eine Datei auf jeder der vier Zeilen angeben. Die Länge der Zeilen ist jedoch auf 80 Zeichen beschränkt. Trennen Sie Pfadnamen innerhalb derselben Zeile durch ein

Option	Beschreibung
	Leerzeichen voneinander ab. Der Scanner vergleicht die Daten und die Größe der aktuellen Datei mit der des vorherigen Scans. Wenn Datum und Größe nicht übereinstimmen, zeichnet der Scan den Inhalt der Datei als neuere Revision auf.
ExcludeDir 1-3	Schließt bestimmte Verzeichnisse aus einem Scan aus. Lassen Sie den Laufwerksbuchstaben (z.B. c:) weg, wenn Sie alle lokalen Laufwerke ausschließen möchten. Aufzählungen müssen mit 1 beginnen und fortlaufend sein. Sie müssen jede Zeile mit "\" beenden.
MifPath	Legt fest, wo MIF-Dateien auf dem lokalen Laufwerk eines Clients gespeichert werden. Der Standardpfad ist c:\DMI\DOS\MIFS.
UseDefaultVersion	Wenn die Einstellung TRUE gewählt wird, meldet der Scanner nur dann eine Übereinstimmung, wenn eine Datei genau mit einem Dateinamens- und Dateigrößeneintrag in LDAPPL3 übereinstimmt (in der Meldung trägt die Version den Namen EXISTS). Dies kann zu falschen Ergebnissen für Anwendungen führen, die einen allgemeinen Dateinamen mit einer unbekannten Anwendung gemeinsam verwenden. In der ursprünglichen Datei LDAPPL3.TEMPLATE ist dieser Parameter auf FALSE festgelegt; d. h., es wird nur dann ein Eintrag hinzugefügt, wenn es sich um eine genaue Übereinstimmung handelt. Wenn der Parameter fehlt, ist die Standardeinstellung TRUE.
SendExtraFileData	Wenn die Einstellung TRUE lautet, werden zusätzliche Dateidaten an den Core Server gesendet. Standard ist FALSE. Dies bedeutet, dass standardmäßig nur Pfad, Name und Version in die Core-Datenbank eingetragen werden.

So bearbeiten Sie die Datei LDAPPL3.TEMPLATE

1. Wechseln Sie von Ihrem Core Server aus in das Verzeichnis \Programme\LANDesk\ManagementSuite\LDLogon und öffnen Sie die Datei LDAPPL3.TEMPLATE in Notepad oder einem anderen Texteditor.
2. Blättern Sie nach unten zu dem Parameter, den Sie aktualisieren möchten, und nehmen Sie die Änderungen vor.
3. Speichern Sie die Datei.

Aktualisieren der Softwareliste

Die Daten aus der Softwareliste DEFAULTS.XML werden in der Core-Datenbank gespeichert. Da sich Name und Versionsnummer häufig verwendeter Softwareprogramme relativ oft ändern, veröffentlicht LANDesk mehrmals jährlich eine neue DEFAULTS.XML (in früheren Versionen von LANDesk Software trug diese Datei den Namen LDAPPL.INI).

So aktualisieren Sie die Softwareliste

1. Laden Sie eine neue DEFAULTS.XML oder LDAPPL3.TEMPLATE von der Website http://www.landesk.com/support/downloads herunter. Wählen Sie ein Produkt aus und klicken Sie auf **Software-Update** um die Datei herunterzuladen.
2. Speichern Sie die Datei im Verzeichnis LDLOGON.
3. Veröffentlichen Sie eine neue LDAPPL3.INI, indem Sie die Schritte unter Veröffentlichen der Softwareliste ausführen.

Veröffentlichen der Softwareliste

Das Veröffentlichen der Softwareliste umfasst das Importieren der neuesten Softwareliste aus der Datei DEFAULTS.XML in die Datenbank und das anschließende Kombinieren der Softwareliste mit dem Inhalt der Datei LDAPPL3.TEMPLATE, um eine aktualisierte LDAPPL3.INI zu erstellen. Es gibt im Verzeichnis \Programme\LANDesk\ManagementSuite ein Standalone-Programm mit dem Namen COREDBUTIL.EXE, mit dem diese Schritte automatisch ausgeführt werden.

So veröffentlichen Sie die Softwareliste

1. Starten Sie CoreDBUtil.exe
2. Klicken Sie auf die Schaltfläche **Softwareliste veröffentlichen**.

Sie sollten die Softwareliste veröffentlichen, nachdem Sie eine aktualisierte Version von LDAPPL3.TEMPLATE oder DEFAULTS.XML geändert oder heruntergeladen haben.

Hardware-Konfiguration

Intel* AMT-Support

System Manager unterstützt Geräte, die Intel* Active Management Technology (Intel* AMT) verwenden. Intel* AMT ist eine Hardware- und Firmware-Funktionalität, die die Verwaltung von Remote-Geräten ermöglicht. Intel AMT verwendet für den Zugriff auf Geräte Out-of-Band-Kommunikation (OOB), unabhängig vom Zustand des Betriebssystems oder der Stromversorgung des Geräts.

Intel AMT-Support in diesem Produkt umfasst Version 1 und 2. Der Prozess für die Bereitstellung auf Intel AMT 2-Geräten schließt mehrere neue Funktionen ein, die in Version 1 nicht enthalten waren. Weitere Informationen zur Bereitstellung mit Version 2 finden Sie unter Konfigurieren von Intel AMT-Geräten. Die Informationen in diesem Abschnitt beziehen sich, soweit nicht anders vermerkt, auf beide Versionen.

Das Tool "Hardware-Konfiguration" beinhaltet folgende Funktionen für die Verwaltung von Intel AMT-Geräten:

- Automatisches Generieren von Bereitstellungskennungen (PID und PPS) (Version 2)
- Ändern des Benutzernamens und Kennworts für verwaltete Geräte
- Konfigurieren und Aktivieren von System Defense-Richtlinien (Version 2)
- Konfigurieren und Aktivieren der Agentenpräsenzüberwachung (Version 2)

Verwalten von Geräten mit oder ohne Verwaltungsagenten

Wenn Geräte mit Intel AMT konfiguriert sind, steht eine begrenzte Anzahl Verwaltungsfunktionen zur Verfügung, auch wenn kein LANDesk Agent auf dem Gerät installiert ist. Solange Geräte mit dem Netzwerk verbunden und mit Standby-Strom versehen sind, können sie erkannt und dem Inventar hinzugefügt werden, um mit anderen Geräten im Netzwerk verwaltet zu werden.

Falls auf einem Gerät Intel AMT aber kein Management Agent installiert ist, kann das Gerät mit der Funktion "Erkennen nicht verwalteter Geräte" erkannt, in die Inventardatenbank verschoben und dann in der Liste **Eigene Geräte** angezeigt werden. Jedoch stehen viele System Manager-Verwaltungsoptionen nicht zur Verfügung. Diese Optionen sind erst dann verfügbar, wenn der LANDesk Agent installiert wird. Für mit Intel AMT konfigurierte Geräte stehen u.a. folgende Verwaltungsfunktionen zur Verfügung:

- **Inventarübersicht:** Ein Teilsatz der normalen Inventardaten kann abgerufen und in Echtzeit für das Gerät angezeigt werden, auch wenn das Gerät ausgeschaltet ist.
- **Ereignisprotokoll:** Ein Protokoll mit Intel AMT-spezifischen Ereignissen, das den Schweregrad und die Beschreibung der Ereignisse anzeigt, kann in Echtzeit angezeigt werden.

- **Remote-Boot-Manager:** Energiezyklus und mehrere Neustartoptionen können von der Remote-Verwaltungskonsole aus gestartet werden, unabhängig vom Zustand des Betriebssystems oder der Stromzufuhr des Geräts. Die verfügbaren Optionen hängen von der Unterstützung der Optionen auf dem Gerät ab. Einige Geräte unterstützen unter Umständen nicht alle Startoptionen.
- **Anfälligkeitsscan erzwingen und Betriebssystemnetzwerk deaktivieren:** Falls schädliche Software auf einem Gerät erscheint, kann ein Anfälligkeitsscan beim nächsten Neustart ausgeführt werden; falls nötig kann der Netzwerkzugriff des Geräts auf der Betriebssystemebene deaktiviert werden, um zu vermeiden, dass ungewünschte Pakete auf dem Netzwerk verteilt werden.

Weitere Informationen zu den Verwaltungsoptionen finden Sie unter Verwalten von Intel AMT-Geräten.

Bereitstellungsanforderungen für Intel AMT, Version 1

Geräte werden erst dann als Intel AMT-Geräte erkannt, nachdem Sie den Intel AMT-Konfigurationsbildschirm auf dem Gerät geöffnet und das Standardkennwort des Herstellers in ein sicheres Kennwort geändert haben. (Weitere Informationen über den Zugriff auf den Intel AMT-Konfigurationsbildschirm finden Sie in der Dokumentation des Herstellers.) Wenn Sie diesen Schritt nicht ausgeführt haben, werden die Geräte zwar erkannt, jedoch nicht als Intel AMT-Geräte identifiziert; darüber hinaus wird nicht dieselbe Inventarübersicht angezeigt, die andernfalls angezeigt würde.

Damit sich der Core Server gegenüber erkannten Intel AMT-Geräten authentifizieren kann, müssen die Berechtigungsnachweise für Benutzername/Kennwort mit den Berechtigungsnachweisen übereinstimmen, die Sie mithilfe der Anwendung "Dienste konfigurieren" konfigurieren. Sie können die Berechtigungsnachweise mithilfe des Intel AMT-Konfigurationsbildschirms ändern.

Wenn ein Intel AMT-Gerät der Core-Datenbank hinzugefügt wird, damit es verwaltet werden kann, wird es von System Manager automatisch in dem Modus bereitgestellt, den Sie im Dienstprogramm "Dienste konfigurieren" auswählen, auch wenn es bereits bereitgestellt wurde. Der Small Business-Modus bietet einfache Verwaltungsfunktionen ohne Netzwerkinfrastrukturdienste (Sicherheitsmodus 1), während der Enterprise-Modus für große Unternehmen vorgesehen ist. Dieser Modus verwendet DHCP, DNS und einen TLS-Zertifikatsautoritätsdienst, der darüber wacht, dass die Kommunikation zwischen verwaltetem Gerät und Core Server sicher ist.

Wenn Sie ein Intel AMT-Gerät im Enterprise-Modus bereitstellen, installiert der Core Server ein Zertifikat für die sichere Kommunikation auf dem Gerät. Wenn das Gerät von einem anderen Core Server verwaltet werden soll, muss die Bereitstellung des Geräts rückgängig gemacht und das Gerät anschließend vom neuen Core Server erneut bereitgestellt werden. Wenn dies nicht geschieht, reagiert der Intel AMT-Zugriff des Geräts nicht, da der neue Core Server kein übereinstimmendes Zertifikat besitzt. Gleichermaßen gilt, dass andere Computer, die versuchen, auf die Intel AMT-Funktionalität zuzugreifen, scheitern werden, da sie kein übereinstimmendes Zertifikat besitzen.

Konfigurieren von Intel* AMT-Geräten

Geräte mit Intel AMT-Funktionen sollten beim ersten Einschalten und Einrichten konfiguriert werden. Die Bereitstellung umfasst mehrere Sicherheitsmaßnahmen, um zu gewährleisten, dass nur berechtigte Benutzer Zugang zu den Intel AMT-Verwaltungsfunktionen erhalten.

Intel AMT-Geräte kommunizieren mit einem Bereitstellungsserver auf dem Netzwerk. Der Bereitstellungsserver wartet auf Nachrichten von Intel AMT-Geräten auf dem Netzwerk und ermöglicht dem IT-Personal die Verwaltung von Servern über Out-of-Band-Kommunikation, unabhängig vom Status des Betriebssystems des jeweiligen Geräts. System Manager agiert als Bereitstellungsserver für Intel AMT-Geräte und umfasst Funktionen, die Ihnen bei der Einrichtung von Geräten zur Bereitstellung behilflich sind. Sie können daraufhin die Geräte mit oder ohne zusätzliche System Manager Verwaltungsagenten verwalten.

Dieser Abschnitt beschreibt ein empfohlenes Verfahren zur Konfiguration neuer Intel AMT-Geräte (Version 2). Bei diesem Verfahren verwenden Sie System Manager, um einen Satz Bereitstellungskennungen (PID und PPS) zu erzeugen. Wenn diese Kennungen in den Intel AMT-Konfigurationsbildschirm des Geräts eingegeben werden, sorgen sie für eine sichere Verbindung mit dem Bereitstellungsserver, dem diese Kennungen bekannt sind, damit das Intel AMT-Gerät seinen anfänglichen Bereitstellungsprozess ausführen kann.

Bei Geräten mit AMT Version 1 ist der Prozess ähnlich, es werden jedoch keine PID- und PPS-Schlüssel verwendet. Detaillierte Informationen hierzu sind in den Hinweisen am Ende dieses Abschnitts zu finden.

Bereitstellung für Intel AMT 2-Geräte

Wenn ein Intel AMT 2-Gerät geliefert wird, wird der Computer vom IT-Techniker zusammengebaut und eingeschaltet. Nach dem Einschalten des Geräts meldet sich der Techniker im BIOS-basierten Intel ME-Konfigurationsbildschirm (Management Engine) an und ändert das Standardkennwort (admin) in ein starkes Kennwort. Dies ermöglicht den Zugriff auf den Intel AMT-Konfigurationsbildschirm.

Im Intel AMT-Konfigurationsbildschirm werden folgende Informationen für die Bereitstellung eingegeben:

- eine Bereitstellungs-ID (PID)
- ein PPS-Schlüssel (auch als Preshared Key oder PSK bezeichnet)
- die IP-Adresse des Bereitstellungsservers
- Anschluss 9982 zur Kommunikation mit dem Bereitstellungsserver
- der Enterprise-Modus sollte ausgewählt sein
- der Host-Name des Intel AMT-Geräts

Der PPS muss dem Bereitstellungsserver und dem verwalteten Gerät bekannt sein, darf aus Sicherheitsgründen jedoch nicht übers Netzwerk übertragen werden. Er muss von Hand in das Gerät eingegeben (im Intel AMT-Konfigurationsbildschirm) und auf dem Bereitstellungsserver gespeichert werden, der in diesem Fall auch der Core Server für System Manager ist. System Manager erzeugt PID/PPS-Paare und speichert diese in der Datenbank. Sie können eine Liste der für die Bereitstellung erzeugten ID-Paare ausdrucken.

Der IT-Techniker sollte die IP-Adresse des System Manager Core Servers als Bereitstellungsserver und Anschluss 9982 angeben. Ansonsten sendet das Intel AMT-Gerät standardmäßig einen allgemeinen Broadcast, der empfangen werden kann, wenn der Konfigurationsserver Anschluss 9971 abhört.

Benutzername und Kennwort (Standard) für den Zugriff auf den Intel AMT-Konfigurationsbildschirm sind "admin" und "admin". Diese werden bei der Bereitstellung geändert. Der Benutzername kann gleich bleiben, aber das Kennwort muss in ein starkes Kennwort geändert werden. Die neue Kombination aus Benutzername und Kennwort wird in das in System Manager enthaltene Dienstprogramm "Dienste konfigurieren" eingegeben (Verfahren siehe unten). Nachdem alle Geräte konfiguriert wurden, können Sie den Benutzernamen bzw. das Kennwort einzeln für jedes Gerät ändern. Für die Bereitstellung müssen Sie jedoch den Benutzernamen/das Kennwort aus dem Dienstprogramm "Dienste konfigurieren" verwenden.

Wenn die oben angegebenen Informationen in den Intel AMT-Konfigurationsbildschirm eingegeben wurden, sendet das Gerät Begrüßungsnachrichten, wenn es zum ersten Mal an das Netzwerk angeschlossen wird und versucht, mit dem Bereitstellungsserver zu kommunizieren. Wenn der Bereitstellungsserver diese Nachricht empfängt, beginnt der Bereitstellungsprozess, sobald der Server eine Verbindung zum verwalteten Gerät herstellt.

Wenn der Core Server die Begrüßungsnachricht empfangen und die PID-/PPS-Schlüssel geprüft hat, stellt er das Intel AMT-Gerät für den TLS-Modus bereit. Der TLS-Modus (Transport Layer Security) stellt einen sicheren Kommunikationskanal zwischen dem Core Server und dem verwalteten Server zur Verfügung, während die Bereitstellung abgeschlossen wird. Bei diesem Prozess wird u. a. ein Datensatz mit der UUID und den verschlüsselten Berechtigungsnachweisen des Geräts in der Datenbank erstellt. Wenn die Daten für das Gerät in der Datenbank abgelegt wurden, erscheint das Gerät in der Liste nicht verwalteter Geräte.

Wenn ein Intel AMT-Gerät vom Core Server bereitgestellt wurde, kann es allein mit den Intel AMT-Funktionen verwaltet werden. Sie können es aus der Liste nicht verwalteter Geräte auswählen und zu Ihren verwalteten Geräten hinzufügen. Oder Sie können System Manager Verwaltungsagenten auf dem Gerät bereitstellen, um einen umfangreicheren Satz an Verwaltungsfunktionen zu verwenden.

Das empfohlene Verfahren zur Verwendung von System Manager zur Bereitstellung von Intel AMT 2-Geräten wird im Folgenden beschrieben. Die folgenden Schritten enthalten spezifische Anweisungen für Version 1 und 2.

1. Geben Sie mithilfe des Dienstprogramms "Dienste konfigurieren" ein neues, starkes Kennwort für die Bereitstellung von Intel AMT-Geräten ein. (Siehe detaillierte Schritte weiter unten.)
2. Verwenden Sie System Manager, um einen Satz Intel AMT-Bereitstellungskennungen (PID und PPS) zu generieren und die Schlüsselliste zu drucken. (Siehe detaillierte Schritte weiter unten.)
3. Melden Sie sich vom BIOS aus im Intel ME-Konfigurationsbildschirm des Geräts an und ändern Sie das Standardkennwort in ein starkes Kennwort.
4. Melden Sie sich im Intel AMT-Konfigurationsbildschirm an. Geben Sie ein PID-/PPS-Schlüsselpaar aus der ausgedruckten Liste von Bereitstellungskennungen ein. Geben Sie die IP-Adresse des Core Servers (Bereitstellungsservers) ein und geben Sie Port 9982 an. Achten Sie darauf, dass für die Bereitstellung der Enterprise-Modus gewählt wurde. Geben Sie den Host-Namen des Intel AMT-Geräts ein.

5. Sobald Sie den BIOS-Bildschirm verlassen, beginnt das Gerät, Begrüßungsnachrichten zu senden.
6. Wenn der Core Server eine solche Begrüßungsnachricht erhält, vergleicht er den PID-/PPS-Schlüssel mit der Liste erzeugter Schlüssel. Bei Übereinstimmung stellt er das Gerät im TLS-Modus bereit.
7. Daraufhin wird das Gerät der Liste nicht verwalteter, erkannter Geräte hinzugefügt.
8. Wählen Sie das Gerät aus und fügen Sie es in Ihre Liste verwalteter Geräte ein. Standardmäßig wird es als Gerät ohne Agent verwaltet. Sie können jedoch auch Verwaltungsagenten dafür bereitstellen.

So stellen Sie den Intel AMT-Benutzernamen und das Kennwort in "Dienste konfigurieren" ein:

1. Klicken Sie vom Core Server aus auf **Start**LANDesk | **Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte **Intel AMT-Konfiguration**.
3. Geben Sie **admin** als Benutzernamen und Kennwort ein unter **Aktuelle Intel AMT-Berechtigungsnachweise**.
4. Geben Sie einen neuen Benutzernamen (optional) und ein starkes Kennwort ein unter **Mit neuen Intel AMT-Berechtigungsnachweisen versorgen**.
5. Klicken Sie auf **OK**.

Die Felder für Benutzername und Kennwort müssen hier ausgefüllt werden, bevor Sie einen Satz Bereitstellungskennungen generieren können.

So erstellen Sie einen Satz Intel AMT-Bereitstellungskennungen:

1. Klicken Sie im linken Navigationsfenster des Core Servers auf **Hardware-Konfiguration**.
2. Erweitern Sie **AMT** und führen Sie einen Drilldown von **Bereitstellung** bis **AMT-Kennungen generieren** durch.
3. Geben Sie die Anzahl der zu generierenden Kennungen ein (in der Regel ist das die Anzahl von Geräten, die bereitgestellt werden sollen).
4. Wenn Sie ein anderes Präfix für die PIDs bevorzugen, geben Sie dieses in das Textfeld **PID-Präfix** ein. Dieses Präfix darf nur Großbuchstaben und Zahlen aus dem ASCII-Zeichensatz enthalten. Es können maximal 7 Zeichen für ein Präfix eingegeben werden.
5. Geben Sie einen Batchnamen ein für diese Gruppe generierter Kennungen.
6. Aktivieren Sie das Kontrollkästchen **Generierte AMT-Kennungen anzeigen**, um die erzeugten Kennungen in der Liste anzuzeigen. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die Kennungen generiert und in der Datenbank gespeichert, jedoch nicht hier angezeigt.
7. Klicken Sie auf **Kennungen generieren**.
8. Wenn die Kennungen generiert wurden, klicken Sie auf **Kennungsliste drucken**, um ein neues Fenster mit der Kennungsliste zu öffnen. (Im neuen Fenster werden nur die derzeit in der Liste enthaltenen Kennungen angezeigt.) Sie können die Liste mit der Druckfunktion Ihres Browsers ausdrucken.
9. Um alle bereits generierten Kennungen anzuzeigen, lassen Sie das Feld **Batchname** leer und klicken Sie auf **Batch-IDs anzeigen**.
10. Um einen Batch von generierten Kennungen anzuzeigen, geben Sie den Batchnamen in das Textfeld **Batchname** ein und klicken Sie auf **Batch-IDs anzeigen**.

Sie können eine beliebige Anzahl von Bereitstellungsschlüsseln auf einmal erstellen. Die Schlüssel werden zum künftigen Gebrauch bei der Bereitstellung neuer Intel AMT-Geräte in der

Datenbank gespeichert. Wenn Geräte bereitgestellt und die Bereitstellungsschlüssel aufgebraucht werden, werden die bereits verbrauchten Kennungen auf der Seite **AMT-Kennungen generieren** schattiert dargestellt, damit Sie den Überblick behalten.

Damit Sie Kennungen leichter als PIDs identifizieren können, wird ein PID-Präfix hinzugefügt. Es muss jedoch nicht verwendet werden. Wir empfehlen 0 bis 4 Zeichen, die Maximalzahl für das Präfix ist 7 Zeichen.

Um Bereitstellungsschlüssel-Batches zu identifizieren, geben Sie einen Batchnamen ein. Dieser Name sollte beschreibend sein und angeben, auf welche Geräte sich die Kennungen beziehen. So können Sie zum Beispiel Batches für jede Organisation innerhalb Ihres Unternehmens generieren und diese als "Entwicklung", "Marketing", "Finanzen" usw. bezeichnen. Wenn Sie später die generierten Kennungen einsehen möchten, geben Sie den Batchnamen ein und klicken auf **Batch-IDs anzeigen**, um eine Liste mit nur diesen Kennungen anzuzeigen.

Starke Kennwörter

Die sichere Kommunikation bei Intel AMT erfordert ein starkes Kennwort. Kennwörter müssen folgende Anforderungen erfüllen:

- Es muss mindestens 8 Zeichen beinhalten.
- Es muss mindestens eine Zahl (0 bis 9) enthalten.
- Es muss mindestens ein nicht alphanumerisches Zeichen (z. B. !, &, %) enthalten.
- Es muss lateinische Groß- und Kleinbuchstaben oder nicht-ASCII-Zeichen enthalten (UTF+00800 und höher).

Bereitstellungsfehler

Wenn Sie einen nicht ordnungsgemäß gepaarten PID- und PPS-Satz eingeben (z. B. der PPS-Schlüssel hätte mit einem anderen PID-Schlüssel gepaart werden sollen), erscheint eine Fehlermeldung im Alarmprotokoll, und die Bereitstellung des betroffenen Geräts wird nicht fortgesetzt. Sie müssen das Gerät neu starten und ein korrektes PID-/PPS-Paar im Intel AMT-Konfigurationsbildschirm eingeben.

Wenn der Intel AMT-Konfigurationsbildschirm bei der Eingabe eines PID-Schlüssels eine Fehlermeldung anzeigt, haben Sie sich beim PID vertippt. Der PID-Schlüssel wird mit einer Prüfsumme überprüft.

Erkennen von Intel AMT 1.0 Geräten

Wenn Sie einen Erkennungs-Scan laufen lassen, werden Geräte der Intel AMT Version 1 erkannt und dem Intel AMT-Ordner in der Liste **nicht verwalteter** Geräte hinzugefügt. Die Geräte werden als Intel AMT-Geräte erkannt, wenn sie mit einem sicheren Benutzernamen und Kennwort konfiguriert wurden, die die werkseitigen Standardeinstellungen ersetzen.

Wenn Sie im Intel AMT-Konfigurationsbildschirm einen Benutzernamen und ein Kennwort (beides sicher) eingeben, können Sie gleichzeitig die IP-Adresse des Bereitstellungsservers eingeben und Anschluss 9982 angeben, genau wie bei Intel AMT 2-Geräten. Zur Bereitstellung von Intel AMT 1-Geräten werden jedoch keine PID-/PPS-Paare verwendet. Wenn Sie eine IP-Adresse für

den Bereitstellungsserver angeben, fungiert der Core Server als Bereitstellungsserver, und sie können das Gerät ohne Agenten verwalten.

Es ist zu beachten, dass Intel AMT Version 1 eine andere Sicherheitsstufe als Version 2 verwendet. Intel empfiehlt, Geräte mit Version 1 auf einem isolierten, sicheren Netzwerk zu konfigurieren. Nach Abschluss der Konfiguration können sie zur Verwaltung auf ein weniger sicheres Netzwerk verlegt werden.

Ändern des Benutzernamens und Kennworts für Intel* AMT-Geräte

Die Bereitstellung neuer Intel AMT-Geräte (Version 1) setzt die Verwendung eines sicheren Benutzernamens und Kennwortes voraus. Für Geräte, die Sie mit System Manager verwalten werden, sollten Benutzername und Kennwort, den/das Sie in den Intel AMT-Konfigurationsbildschirm eingeben, mit dem Benutzernamen und Kennwort übereinstimmen, den/das Sie in das Programm "Dienste konfigurieren" von System Manager eingegeben haben. Benutzername und Kennwort im Programm "Dienste konfigurieren" werden in der Datenbank gespeichert und global bei der Versorgung von Intel AMT-Geräten angewendet.

Die sichere Kommunikation bei Intel AMT erfordert ein starkes Kennwort. Kennwörter sollten folgende Anforderungen erfüllen:

- Es muss mindestens 8 Zeichen beinhalten.
- Es muss mindestens eine Zahl (0 bis 9) enthalten.
- Es muss mindestens ein nicht alphanumerisches Zeichen (z. B. !, &, %) enthalten.
- Es muss lateinische Groß- und Kleinbuchstaben oder nicht-ASCII-Zeichen enthalten (UTF+00800 und höher).

Nach der Bereitstellung sollten Sie die Benutzernamen und Kennwörter als Teil Ihres IT-Wartungsplans regelmäßig ändern. Sie können für jedes Intel AMT-Gerät eine andere Kombination aus Benutzername/Kennwort verwenden oder eine Benutzername/Kennwort-Kombination auf mehrere Geräte anwenden. Die von Ihnen auf der Seite "Hardware-Konfiguration" eingegebenen Benutzername/Kennwort-Kombinationen werden in der Datenbank gespeichert und von System Manager für die sichere Kommunikation mit verwalteten Intel AMT-Geräten verwendet.

So ändern Sie den Benutzernamen und das Kennwort für Intel* AMT-Geräte

1. Klicken Sie im linken Navigationsfenster des Core Servers auf **Hardware-Konfiguration**.
2. Erweitern Sie **AMT** und führen Sie einen Drilldown bis **Konfiguration** aus.
3. Wählen Sie in der Liste **Alle Geräte** mindestens ein Gerät aus, für das Sie den Benutzernamen und das Kennwort ändern möchten. Klicken Sie in der Symbolleiste auf **Ziel**.
4. Geben Sie im unteren Bereich den neuen Benutzernamen ein. Geben Sie dann das Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **Zielcomputer** und dann auf **Übernehmen**.

   Für ein einzelnes oder mehrere Geräte in derselben Liste können Sie die Geräte auswählen und auf **Ausgewählte Geräte** sowie anschließend auf **Übernehmen** klicken.

Konfigurieren von System Defense-Richtlinien

Intel AMT* 2.0 beinhaltet eine System Defense-Funktion, die Netzwerksicherheitsrichtlinien auf Geräten mit Intel AMT 2.0-Funktionalität durchsetzt. Zum Auswählen und Anwendungen von System Defense-Richtlinien für verwaltete Geräte verwenden Sie das Tool **Hardware-Konfiguration**.

Wenn eine System Defense-Richtlinie auf ein Intel AMT-Gerät angewendet wird, filtert das Gerät eingehende und ausgehende Netzwerkwerkpakete in Übereinstimmung mit den definierten Richtlinien. Wenn Netzwerkdaten den in einem Filter definierten Alarmbedingungen entsprechen, wird ein Alarm generiert und der Netzwerkzugriff des Geräts gesperrt. Das Gerät wird dann solange vom Netzwerk isoliert, bis Sie die Reparaturschritte für die betreffende Richtlinie ausgeführt haben.

System Manager enthält vordefinierte System Defense-Richtlinien, die Sie auf Ihre Intel AMT-Geräte anwenden können. Jede Richtlinie enthält eine Gruppe von Filtern, mit denen festgelegt wird, welche Netzwerkdaten nicht zugelassen werden und welche Maßnahmen zu ergreifen sind, wenn die Daten den Kriterien des Filters entsprechen. Richtlinien werden wie folgt ausgewählt und angewendet:

1. Wählen Sie mindestens ein verwaltetes Gerät als Zielgerät aus.
2. Wählen Sie die anzuwendende System Defense-Richtlinie aus; bearbeiten Sie nach Bedarf die Richtlinie.
3. Wenden Sie die Richtlinie auf Zielgeräte an.

Wenn eine System Defense-Richtlinie auf einem verwalteten Gerät aktiv ist, überwacht das Gerät alle ein- und ausgehenden Netzwerkdaten. Wenn Filterbedingungen erkannt werden, geschieht Folgendes:

1. Das verwaltete Gerät sendet einen ASF-Alarm an den Core Server und das Alarmprotokoll wird um einen Eintrag erweitert.
2. Der Core Server stellt fest, gegen welche Richtlinie verstoßen wurde, und sperrt den Netzwerkzugriff auf verwalteten Geräten.
3. Das Gerät wird in der System Defense-Reparaturschlange aufgelistet (im Tool **Hardware-Konfiguration**).
4. Um den Netzwerkzugriff auf dem Gerät wiederherzustellen, führt der Administrator die erforderlichen Reparaturschritte aus und entfernt dann das Gerät aus der Reparaturwarteschlange; damit wird die ursprüngliche System Defense-Richtlinie auf dem Gerät wiederhergestellt.

Dieser Ablauf wird in den nachfolgenden Abschnitten ausführlich beschrieben.

Auswählen und Anwenden von System Defense-Richtlinien

System Managerenthält die folgenden vordefinierten auf Intel AMT 2.0-Geräte anwendbaren System Defense-Richtlinien. Richtlinien werden mit Parametern wie Anschlussnummer, Pakettyp und Paketanzahl während einer festgelegten Zeitspanne definiert. Wenn Sie eine Richtlinie

aktivieren, wird diese auf den von Ihnen ausgewählten Geräten bei Intel AMT angemeldet. Richtlinien werden als XML-Dateien im Ordner "CircuitBreakerConfig" auf dem verwalteten Gerät gespeichert.

- **BlockFTPSrvr:** Diese Richtlinie verhindert die Übermittlung von Netzwerkdaten über einen FTP-Anschluss. Pakete, die von FTP-Anschluss 21 gesendet bzw. dort in Empfang genommen werden, werden verworfen und der Netzwerkzugriff wird unterbrochen.
- **LDCBKillNics:** Diese Richtlinie blockiert Netzwerkdaten an allen Anschlüssen, mit Ausnahme der folgenden Verwaltungsanschlüsse:

Beschreibung des Anschlusses	Zahlenbereich	Datenrichtung	Protokoll
LANDesk Management	9593-9595	Senden/Empfangen	TCP, UDP
Intel AMT Management	16992-16993	Senden/Empfangen	Nur TCP
DNS	53	Senden/Empfangen	Nur UDP
DHCP	67-68	Senden/Empfangen	Nur UDP

Wenn der Core Server den Netzwerkzugriff auf einem verwalteten Gerät deaktiviert, bedeutet dies, dass diese Richtlinie auf das Gerät angewendet wird. Wird dann das Gerät aus der Reparaturschlange entfernt, so wird die ursprüngliche Richtlinie erneut auf das Gerät angewendet.

- **LDCBSYNFlood:** Diese Richtlinie erkennt einen SYN-Flut Denial-of-Service-Angriff. Sie unterstützt maximal 10.000 TCP-Pakete mit eingeschaltetem SYN-Flag pro Minute. Bei Überschreitung dieses Wertes wird der Netzwerkzugriff deaktiviert.
- **UDPFloodPolicy:** Diese Richtlinie erkennt einen UDP-Flut Denial-of-Service-Angriff. Sie lässt mehr als 20.000 UDP-Pakete pro Minute auf Anschlüssen mit der Zahl 0 bis 1023 zu. Bei Überschreitung dieses Wertes wird der Netzwerkzugriff deaktiviert.

So wählen Sie eine System Defense-Richtlinie aus

1. Klicken Sie im linken Navigationsfenster auf **Hardware-Konfiguration**.
2. Klicken Sie auf **AMT** und führen Sie einen Drilldown in der Baumansicht aus, bis **Richtlinien** angezeigt wird.
3. Wählen Sie in der Liste mit den Geräten die Geräte aus, auf die Sie die Richtlinie anwenden möchten (verwenden Sie STRG+Mausklick oder UMSCHALT+Mausklick, um mehrere Geräte auszuwählen).
4. Klicken Sie in der Symbolleiste auf **Ziel**, um die Geräte der Liste **Zielgeräte** hinzuzufügen.
5. Wählen Sie im unteren Fensterbereich eine Richtlinie aus der Dropdown-Liste aus.
6. Klicken Sie auf **Zielgeräte** und dann auf **Anwenden**.

Wiederherstellen von Netzwerkzugriff auf Geräten in der Reparaturschlange

Wenn der Netzwerkzugriff eines Geräts aufgrund einer System Defense-Richtlinie deaktiviert wurde, wird das betreffende Gerät in der Reparaturschlange aufgelistet. Das Gerät bleibt so lange in der Liste, bis Sie es aus der Liste entfernen und dadurch die aktive Richtlinie auf diesem Gerät wiederhergestellt wird. Bevor Sie diesen Schritt ausführen, müssen Sie das Problem beheben, dass dafür verantwortlich war, dass das Gerät der Reparaturschlange hinzugefügt wurde. Wurden beispielsweise FTP-Daten erkannt, müssen Sie sicherstellen, dass die entsprechenden Maßnahmen ergriffen werden, um weiteren FTP-Datenverkehr auf dem Gerät zu verhindern.

So entfernen Sie ein Gerät aus der Reparaturschlange.

1. Klicken Sie im linken Navigationsfenster auf **Hardware-Konfiguration**.
2. Klicken Sie auf **AMT** und führen Sie einen Drilldown in der Baumansicht aus, bis **Remediation** angezeigt wird.
3. Wählen Sie die Geräte aus, deren ursprüngliche System Defense-Richtlinie wiederhergestellt werden kann, und klicken Sie auf **Entfernen**.

Intel* AMT Agent Presence-Konfiguration

Intel* AMT 2.0 umfasst ein Agent Presence-Sicherheitstool, mit dem sich die Präsenz von Softwareagenten auf verwalteten Geräten überwachen lässt. Sie können die Agent Presence-Überwachung aktivieren, um sicherzustellen, dass Verwaltungsagenten auf Ihren Geräten fortlaufend ausgeführt und Sie benachrichtigt werden, wenn ein Agent nicht mehr ausgeführt wird. Diese Alarmierung funktioniert sogar dann, wenn andere Software-gestützte Agenten das Problem nicht erkennen.

System Manager überwacht mithilfe von Intel AMT Agent Presence zwei Agenten: Den Standard Management Agent und den Überwachungsdienst. Dieses Verfahren erweist sich als nützlich, wenn keine normale Überwachungskommunikation verfügbar ist. So kann es beispielsweise sein, dass die Kommunikationsschicht eines Geräts nicht funktionsfähig oder der eigentliche Überwachungsagent ausgefallen ist. Agent Presence überwacht standardmäßig auch seine eigenen Überwachungsprozess, sodass Sie benachrichtigt werden, sobald Agent Presence ausfällt.

Die Agent Presence-Überwachung wird mithilfe eines Timers gesteuert, der "Heartbeat"-Nachrichten von auf dem Gerät installierten Verwaltungsagenten abhört, um sicherzustellen, dass die Agenten ausgeführt werden. Wenn ein Timer abläuft, weil ihm keine Heartbeat-Nachrichten mehr zugestellt wurden, alarmiert Intel AMT den Core Server.

Beim Einrichten der Agent Presence-Konfiguration meldet sich der auf dem Gerät installierte Agent bei Intel AMT für die direkte Übermittlung von Heartbeats an Intel AMT an; bleiben die Heartbeats aus, so kann Intel AMT den Core Server über Out-of-Band-Kommunikation informieren, dass der Geräteagent nicht mehr reagiert. Intel AMT sendet einen PET-Alarm (Platform Event Trap) an den Core Server mit einer Beschreibung des geänderten Status. Dieser Alarm wird standardmäßig im Gerätezustand protokolliert. Sie können andere Alarmaktionen konfigurieren und festlegen, dass diese Aktionen bei Zustellung der entsprechenden

Alarmnachricht initiiert werden (weitere Informationen zum Konfigurieren von Alarmaktionen finden Sie unter Konfigurieren von Alarmaktionen).

Beim Konfigurieren der Agent Presence-Überwachung können Sie die Überwachung für zwei Agenten aktivieren oder deaktivieren und folgende Werte festlegen:

- **Heartbeat:** Die maximale Zeitspanne (in Sekunden), die zwischen zwei Heartbeat-Signalen verstreichen darf. Wird dieses Zeitlimit überschritten, ohne dass ein neuer Heartbeat zugestellt wird, so gilt der Agent als nicht reagierend. Der Standardwert ist 120 Sekunden für den Standard Management Agent und 180 Sekunden für den Überwachungsdienst; der Mindestwert für beide ist 30 Sekunden.
- **Startzeit:** Die maximal zulässige Zeitspanne (in Sekunden), die nach dem Starten des Betriebssystems verstreichen darf, bevor ein Heartbeat vom Agenten zugestellt werden muss. Wenn das Zeitlimit überschritten wird, gilt der Agent als nicht reagierend. Agent Presence wird beim Installieren des Agenten auf Intel AMT konfiguriert. Es sollte daher genügend Zeit vorhanden sein, den Agenten zu starten und einen ersten Heartbeat zu senden. Der Standardwert ist 360 Sekunden; der Minimalwert ist 30 Sekunden.

So bearbeiten Sie die Intel AMT Agent Presence-Konfiguration

1. Klicken Sie im linken Navigationsfenster auf **Hardware-Konfiguration**.
2. Erweitern Sie **AMT** und führen Sie einen Drilldown in der Baumansicht aus, bis **AP-Konfiguration** angezeigt wird.
3. Um die Agent Presence-Überwachung auf Intel AMT 2.0-Geräten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Agent Presence-Überwachung aktivieren**.
4. Um die Überwachung für einen bestimmten Agenten zu deaktivieren, deaktivieren Sie das Kontrollkästchen neben dem Namen des Agenten. (Selbst wenn beide Kontrollkästchen deaktiviert sind, setzt Agent Presence die Überwachung seines eigenen Überwachungsprozesses so lange fort, solange er aktiviert ist.)
5. Geben Sie einen neuen Wert in das Textfeld **Heartbeat** ein, um die maximal zulässige Zeitspanne zwischen den einzelnen Heartbeats (mindestens 30 Sekunden) zu ändern.
6. Geben Sie einen neuen Wert in das Feld **Startzeit** ein, um festzulegen, wie viel Zeit maximal verstreichen darf, bis der Agent nach dem Start des Betriebssystems auf dem Gerät den ersten Heartbeat übermittelt (Minimum 30 Sekunden; 120 Sekunden wird empfohlen).

IPMI-Support

System Manager unterstützt IPMI (Intelligent Platform Management Interface) 1.5 und 2.0. IPMI ist eine von Intel,* H-P,* NEC* und Dell* entwickelte Norm, die die Nachrichten- und Systemschnittstelle für verwaltbare Hardwarebestandteile definiert. IPMI enthält Überwachungs- und Wiederherstellungsfunktionen, mit denen Sie auf zahlreiche Funktionen zugreifen können, unabhängig davon, ob der Rechner eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet. Weitere Details zu IPMI erhalten Sie auf Intels Website.

Die IPMI-Überwachung wird vom Baseboard Management Controller (BMC) verwaltet. BMC läuft mit Standby-Strom und ruft selbstständig Daten zum Systemzustand ab. Sie können die Gegenmaßnahmen konfigurieren, die von IPMI eingeleitet werden, wenn BMC erkennt, dass die Werte eines Elements außerhalb des gültigen Bereichs liegen. Zu diesen Maßnahmen gehört beispielsweise das Aufzeichnen des Ereignisses in einem Protokoll, das Erstellen von

Warnmeldungen oder Ausführen automatischer Wiederherstellungsaktionen (System herunterfahren oder zurücksetzen usw.).

Damit BMC auf dem System erkannt wird, muss SMBIOS 2.3.1 oder höher installiert sein. Wird BMC nicht erkannt, sehen Sie möglicherweise keine IPMI-Informationen in Berichten, Exportvorgängen usw.

IPMI definiert Schnittstellen für Hardwarebestandteile, die zur Überwachung von Kontrollsignalen für den Systemzustand verwendet werden (beispielsweise Temperatur, Versorgungsspannung, Lüfter, Stromzufuhr und unbefugtes Öffnen von Gehäusen). Neben den Leistungen zur Überwachung des Systemzustands bietet IPMI Systemverwaltungsfunktionen wie automatische Warnmeldungen, automatisches Herunterfahren und Neustarten des Systems, ferngesteuerter Neustart und Stromverwaltungslösungen sowie Inventarüberwachung.

Was die Optionen im System Manager-Menü betrifft, gibt es für IPMI-kompatible Geräte je nach Betriebssystemzustand geringfügige Unterschiede zu beachten.

Verwaltungsfunktionen für IPMI-kompatible Geräte

Welche Überwachungsfunktionen unterstützt werden, hängt davon ab, welche Komponenten auf dem überwachten Gerät installiert wurden und in welchem Zustand sich das Gerät befindet. Jedes IPMI-aktivierte Gerät, das über einen Baseboard Management Controller (BMC) verfügt, kann von der Verwaltungskonsole in begrenztem Umfang ohne zusätzliche Verwaltungsagenten überwacht werden, nachdem der BMC konfiguriert wurde. Dies schließt die Out-of-Band-Verwaltung ein, wenn das Gerät heruntergefahren wird oder das Betriebssystem nicht funktionsfähig ist. Das komplette Spektrum an Verwaltungsfunktionen ist verfügbar, wenn folgende Bedingungen erfüllt sind: Der Management Agent ist installiert, ein BMC ist vorhanden, das Gerät ist eingeschaltet und das Betriebssystem ist funktionsfähig. Die folgende Tabelle vergleicht die verfügbare Funktionalität in unterschiedlichen Konfigurationen.

	Nur BMC*	**BMC + Agent**	**Agent (kein IPMI)**
Für Out-of-Band-Verwaltung konfiguriert	X	X	
Für In-Band-Verwaltung konfiguriert		X	X
Gerät wird erkannt**	X	X	X
Umgebungssensoren lesen	X	X	Hardwareabhängig
Ein-/Ausschalten aus der Ferne	X	X	X

	Nur BMC*	**BMC + Agent**	**Agent (kein IPMI)**
Ereignisprotokoll lesen & löschen	X	X	
Alarmmeldungen konfigurieren	X	X	X
Betriebssysteminformationen lesen		X	X
Vorschriftsmäßiges Herunterfahren		X	X
SMBIOS-Informationen lesen (Prozessor, Einschübe, Speicher)		X	X
IP-Syncing (Betriebssystem nach BMC)		X	
Watchdog-Timer		X	
BMC kommuniziert mit Core Server	X	X	
Lokale System Manager-Komponenten kommunizieren mit dem Core Server		X	X
Komplettes Spektrum von System Manager-Verwaltungsfunktionen		X	

*Standard BMC. Mini-BMC ist eine abgespeckte Version eines Baseboard Management Controllers. Es verfügt über die oben aufgeführten Funktionen mit Einschränkungen in den folgenden Bereichen:

- Unterstützt keine Serielle over LAN (SOL)-Umleitung
- Besitzt nur einen Benutzernamen für BMC Management
- Verwendet nur einen Kanal für die Kommunikation mit dem BMC
- Verfügt über einen kleineren System Event Log (SEL)-Pool

**Wenn der BMC nicht konfiguriert ist, reagiert er nicht auf ASF-Pings; diese Pings werden vom Produkt für die IPMI-Erkennung verwendet. Das heißt, dass Sie das Produkt als normalen Computer erkennen lassen müssen. Beim Bereitstellen eines Verwaltungsagenten durchsucht die ausführbare Datei der Serverkonfiguration das System, erkennt es als IPMI und konfiguriert den BMC.

Konflikte mit anderen IPMI-Treibern

Wenn Sie andere Verwaltungslösungen (mit integrierten IPMI-Treibern) auf Geräten installiert haben, die Sie mit System Manager verwalten möchten, müssen Sie diese Produkte deinstallieren, bevor Sie Management Suite-Agenten mit IPMI-Verwaltungsfunktionen bereitstellen können.

Beispiel: Microsoft* Windows* Server 2003 enthält IPMI-Support über die Installation von Windows Remote Management (WinRM), wobei WinRM einen Windows Management Instrumentation (WMI)-Provider und einen IPMI-Treiber enthält. System Manager unterstützt jedoch die Installation dieses IPMI-Treibers nicht und installiert einen eigenen IPMI-Treiber. Wenn WinRM auf einem Gerät installiert wurde, das Sie mit System Manager verwalten möchten, müssen Sie zuerst WinRM unter Windows/Software deinstallieren (**Start | Systemsteuerung | Software | Windows-Komponenten hinzufügen/entfernen | Verwaltungs- und Überwachungsprogramme |**, das Kontrollkästchen **Hardwareverwaltung** deaktivieren | auf **OK** klicken).

IPMI BMC-Konfiguration

Verwenden Sie die Seite **IPMI BMC-Konfiguration**, um die Einstellungen für die Kommunikation mit IPMI-tauglichen Geräten anzupassen. Die unten beschriebenen Funktionen stehen für In-Band-Geräte zur Verfügung; bei Out-of-Band-Geräten stehen nur die Stromkonfiguration und die BMC-Benutzereinstellungen zur Verfügung.

VORSICHT: Es wird dringend davon abgeraten, IPMI-Einstellungen zu ändern, es sei denn, Sie sind mit der IPMI-Spezifikation vertraut und kennen die mit diesen Einstellungen verknüpften Technologien. Die unsachgemäße Verwendung dieser Konfigurationsoptionen kann dazu führen, dass System Manager nicht wie erwartet mit den IPMI-kompatiblen Geräten kommuniziert.

Die folgenden Konfigurationsoptionen stehen zur Verfügung:

- Watchdog-Timer
- Energiekonfiguration
- Benutzereinstellungen
- BMC-Kennwort
- LAN-Konfiguration
- SOL-Konfiguration
- IMM-Konfiguration

Ändern der Einstellungen für den Watchdog-Timer

IPMI stellt eine Schnittstelle für den BMC-Watchdog-Timer bereit. Dieser Timer kann so eingestellt werden, dass er periodisch abläuft; er ist so konfiguriert, dass mit seinem Ablaufen

bestimmte Aktionen ausgeführt werden (beispielsweise "Energiezyklus"). System Manager ist dafür konfiguriert, den Timer periodisch zurückzusetzen, damit er nicht abläuft; wenn das Gerät nicht mehr verfügbar ist (z. B. weil es heruntergefahren wurde oder ausgefallen ist), wird der Timer nicht zurückgesetzt und läuft ab, wodurch dann die Aktion ausgelöst wird.

Sie können angeben, wie viel Zeit verstreichen darf, bevor der Timer abläuft, und Sie können eine Aktion auswählen, die ausgeführt wird, wenn er abläuft. Sie können entweder auf die Ausführung einer Aktion verzichten, einen Hard Reset ausführen (Gerät herunterfahren und neu starten), das Gerät ordnungsgemäß herunterfahren oder einen Energiezyklus ausführen (das Gerät ordnungsgemäß herunterfahren und dann erneut starten).

Sie können den BMC auch so konfigurieren, dass keine weitere ARP (Address Resolution Protocol)-Meldungen gesendet werden, während der Watchdog-Timer aktiviert ist. Hiermit kann das Aufkommen an Netzwerkdaten reduziert werden. Wenn Sie die ARPs einstellen, werden diese automatisch fortgesetzt, wenn der Watchdog-Timer abläuft.

So ändern Sie die Einstellungen für den Watchdog-Timer

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Watchdog-Timer**.
4. Aktivieren Sie das Kontrollkästchen **Watchdog-Zeitgeber starten**, um den Timer zu aktivieren.
5. Geben Sie an, wie oft der Timer überprüft werden soll (Anzahl von Minuten oder Sekunden).
6. Wählen Sie eine Aktion aus, die initiiert wird, sobald der Timer abläuft.
7. Wenn Sie BMC am Senden weiterer ARP-Meldungen hindern möchten (während der Watchdog-Timer aktiviert ist), aktivieren Sie das Kontrollkästchen **BMC ARPs aufheben**.
8. Klicken Sie auf **Übernehmen**.
9. Wenn Sie die Einstellungen für den Watchdog-Timer geändert haben, können Sie die Standardeinstellungen wiederherstellen, indem Sie auf **Standardeinstellungen wiederherstellen** klicken.

Ändern der Einstellungen für die Stromkonfiguration

Wenn es auf einem IPMI-kompatiblen Computer zu einem Stromausfall kommt, können Sie festlegen, welche Maßnahme beim Wiederherstellen der Stromzufuhr ergriffen werden sollen. Es wird empfohlen, den Computer in dem Zustand wiederherzustellen, in dem er sich zum Zeitpunkt des Stromausfalls befand. Sie können jedoch auch festlegen, dass der Computer ausgeschaltet bleiben soll oder immer hochgefahren werden soll.

So ändern Sie die Einstellungen für die Stromkonfiguration

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Stromkonfiguration**.

4. Wählen Sie eine Option aus, die beim Wiederherstellen der Stromzufuhr aktiviert werden soll.
5. Klicken Sie auf **Übernehmen**.
6. Wenn Sie die Einstellungen für die Stromkonfiguration geändert haben, können Sie die Standardeinstellungen wiederherstellen, indem Sie auf **Standardeinstellungen wiederherstellen** klicken.

Ändern von BMC-Benutzereinstellungen

System Manager authentifiziert sich gegenüber einem BMC mit einer für den BMC eindeutigen Benutzername/Kennwort-Kombination (separat von allen anderen System Manager-Benutzernamens). System Manager reserviert den ersten Benutzernamen, damit er immer mit dem BMC kommunizieren kann. Wenn der BMC das Definieren anderer Benutzernamen unterstützt, können Sie Benutzernamen mit Kennwörtern für die BMC-Authentifizierung definieren.

Sie können auch Privilegebenen für die einzelnen Benutzer angeben. Für erweiterte IMMs können Sie pro Kanal Protokoll-Privilegebenen angeben (telnet, http und https).

VORSICHT: Gehen Sie äußerst umsichtig vor, wenn Sie diese Einstellungen ändern. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

So ändern Sie BMC-Benutzereinstellungen

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Benutzereinstellungen**.
4. Um die Daten für einen Benutzernamen zu löschen, klicken Sie auf die Indexzahl und dann auf **Löschen**.
5. Klicken Sie zum Hinzufügen oder Ändern eines Benutzernamens auf die Indexzahl und dann auf **Bearbeiten**.
6. Geben Sie einen Benutzernamen ein.
7. Um ein Kennwort festzulegen, aktivieren Sie das Kontrollkästchen **Kennwort festlegen**, geben dann das Kennwort ein und bestätigen es.
8. Wählen Sie die Privilegebenen für LAN-Zugriff und seriellen Zugriff aus.
9. Klicken Sie auf **Änderungen speichern**.

Ändern des BMC-Kennworts

System Manager authentifiziert sich gegenüber dem BMC eines Geräts mithilfe des Standardbenutzernamens (Benutzer 1) und Kennworts. Der Benutzername kann nicht geändert werden, sondern nur das Kennwort. Wenn Sie diese Kennworteinstellung ändern, wird die Änderung in der Datenbank auf dem BMC gespeichert.

So ändern Sie das BMC-Standardkennwort

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Kennwort**.
4. Geben Sie das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **Übernehmen**.

Ändern der LAN-Konfigurationen

IPMI-Meldungen können direkt vom BMC über eine LAN-Schnittstelle (zusätzlich zur Systemschnittstelle des Geräts) übermittelt werden. Das Aktivieren der LAN-Kommunikation ermöglicht es dem Core Server, IPMI-spezifische Warnungen zu empfangen, selbst wenn das Gerät heruntergefahren wurde. Der Core Server hält diese Kommunikationsverbindung aufrecht, solange das Gerät über eine physikalische Netzwerkverbindung mit einer gültigen Netzwerkadresse verfügt, und solange die Hauptstromzufuhr des Geräts eingeschaltet bleibt.

VORSICHT: Wenn Sie die benutzerdefinierte Konfiguration für die LAN- oder serielle Kommunikation auf den BMC festlegen, sollten Sie beim Ändern der Einstellungen mit äußerster Vorsicht vorgehen. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

Wenn Sie über einen definierten LAN-Kanal verfügen, können Sie die Standardeinstellungen für den BMC des Geräts verwenden oder die Einstellungen für IP-Adresse und Gateway ändern. Verwenden Sie diese Optionen, um Ziele für die SNMP-Traps zu konfigurieren, die vom BMC für jede Plattformereignis-Trap (PET, Platform Event Trap) gesendet werden.

Sie können auch die Einstellungen für das Senden von Alarmen über LAN in den Einstellungen für den SNMP Community String ändern. Beim Konfigurieren dieser Einstellungen müssen Sie den für die SNMP-Authentifizierung verwendeten SNMP Community String angeben. Sie können für jede Konfiguration die Informationen zum Trap-Ziel bearbeiten, um anzugeben, wo und wie Traps gesendet und ob sie bestätigt werden.

So legen Sie Eigenschaften für die LAN-Channel-Konfiguration fest

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **LAN-Konfiguration**.
4. Wählen Sie in der Dropdown-Liste "LAN-Kommunikation" die Option **Immer verfügbar** aus, um den Zugriff auf den BMC offen zu halten. Wenn Sie **Deaktiviert** auswählen, haben Sie keinen LAN-Zugriff auf den BMC, wenn das Gerät out-of-band ist.
5. Wählen Sie die Benutzerprivilegien für den Kanal aus: **Administratorrechte** erteilt Zugriff auf alle Befehle, während **Benutzerrechte** nur Lesezugriff erteilt (bei Verwendung von "Benutzerrechte" wird nur eine eingeschränkte Funktionsgruppe bereitgestellt).

6. Aktivieren Sie **BMC ARPs dauerhaft deaktivieren (reduziert Netzwerkverkehr)**, um die vom BMC ausgehenden Address Resolution Protocol-Meldungen auszuschalten. Damit wird zwar das Aufkommen an Netzwerkdaten reduziert, jedoch möglicherweise auch die Kommunikation mit dem BMC verhindert, wenn das Gerät out-of-band ist.
7. Aktivieren Sie **ARP-Antworten ausschalten**, um den BMC am Senden von ARP-Meldungen zu hindern, wenn das Betriebssystem nicht verfügbar ist. Wenn Sie diese Einstellung aktivieren, verhindern Sie möglicherweise die Kommunikation mit dem BMC, wenn das Gerät ausgeschaltet ist.
8. IP-Einstellungen für den LAN-Kanal werden automatisch festgelegt, wenn der BMC mit dem Betriebssystemkanal synchronisiert ist. Falls nicht, ist das Kontrollkästchen der Registerkarte **IP-Einstellungen** aktiviert. Sie können die Aktivierung des Kontrollkästchens beibehalten, um automatisch bereitgestellte DHCP-Einstellungen zu verwenden; oder Sie können das Kontrollkästchen deaktivieren und die Textfelder mit statischen Einstellungen bearbeiten. Im Allgemeinen ist der Verwendung der automatischen Einstellungen der Vorzug zu geben.
9. Klicken Sie auf die Registerkarte **Alarme über LAN senden**, um die Einstellungen für den SNMP Community String zu konfigurieren (siehe Details weiter unten).
10. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

So ändern Sie die Einstellungen für "Alarme über LAN senden"

1. Öffnen Sie die Seite **LAN-Konfiguration** (Schritte 1-3 oben).
2. Klicken Sie auf die Registerkarte **Alarme über LAN senden**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Senden von SNMP-Alarmen zu ermöglichen.
4. Geben Sie den für die SNMP-Authentifizierung zu verwendenden **SNMP Community String** an.
5. Doppelklicken Sie zum Konfigurieren der Trap-Ziele auf die Indexzahl, um das Dialogfeld **Eigenschaften** zu öffnen.
6. Geben Sie die IP-Adresse an, an die der BMC Alarmmeldungen senden wird, und geben Sie die entsprechende MAC-Adresse an.
7. Geben Sie die Anzahl der Wiederholungsversuche, die Häufigkeit der Wiederholungen und das bevorzugt zu verwendende Gateway an.
8. Wenn Sie veranlassen möchten, dass die Alarmmeldungen bestätigt werden (verursacht ein erhöhtes Aufkommen an Netzwerkdaten), aktivieren Sie das Kontrollkästchen **Alarme bestätigen**.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf der Seite "LAN-Konfiguration" auf **Übernehmen**, nachdem alle Einstellungen vollständig angegeben wurden.

Ändern der Serial Over LAN (SOL)-Konfigurationen

Verwenden Sie SOL (Serial Over LAN), um serielle Modemeinstellungen für bestimmte Verwendungszwecke anzupassen, beispielsweise das Umleiten von BIOS POST-Nachrichten an den seriellen Anschluss. Wenn der BMC über eine Modemverbindung nach außen wählen muss, müssen außerdem spezifische Modemeinstellungen wie Initialisierungs- und Wählzeichenfolgen angegeben werden.

Für seriellen Modembetrieb müssen Sie möglicherweise die BIOS- und Jumper-Einstellungen der Geräteplatine konfigurieren. Weitere Informationen finden Sie in der Dokumentation des entsprechenden Geräts.

VORSICHT: Wenn Sie die benutzerdefinierte Konfiguration für die LAN- oder serielle Kommunikation auf den BMC festlegen, sollten Sie beim Ändern der Einstellungen mit äußerster Vorsicht vorgehen. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

So ändern Sie die SOL-Konfigurationseinstellungen

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **SOL-Konfiguration**.
4. Aktivieren Sie **Serial-Over-LAN-Kommunikationen einschalten**, um SOL zu aktivieren.
5. Wählen Sie **Benutzerebene erforderlich, um SOL zu aktivieren** zum Festlegen der mindestens erforderlichen Benutzerebene.
6. Wählen Sie die **Baudrate für SOL-Sitzungen**, die zur Hardware-Konfiguration des Geräts passt.
7. Klicken Sie auf **Übernehmen**.

Ändern von IMM-Konfigurationen

Die Seite **IMM-Konfiguration** wird nur für IPMI-Geräte angezeigt, die über eine erweiterte IMM Add-in-Karte verfügen. Mit den Optionen auf dieser Seite können Sie Protokolle und Funktionen zur Verwendung mit dem IMM-tauglichen Gerät aktivieren oder deaktivieren. Konsultieren Sie die Dokumentation des IMM-Herstellers, bevor Sie diese Einstellungen ändern.

So ändern Sie IMM-Konfigurationseinstellungen

1. Doppelklicken Sie in der Ansicht **Eigene Geräte** auf das Gerät, das Sie konfigurieren möchten.
2. Klicken Sie im linken Navigationsfenster der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **IMM-Konfiguration**.
4. Aktivieren Sie die Kontrollkästchen für Protokolle und Funktionen, die Sie aktivieren möchten, und fügen Sie alle etwaigen erforderlichen Einstellungen hinzu. Zu den verfügbaren Optionen gehören:
    - KVM
    - SNMP
    - telnet
    - SMTP-Alarmierung
    - HTTP
    - HTTPS
5. Klicken Sie auf **Übernehmen**.

Verwalten von Dell* DRAC-Geräten

Dieses Produkt umfasst eine Management-Integrationsfunktion mit Geräten, die mit einem Dell* DRAC (Remote Access Controller) ausgestattet sind. Der DRAC ist ein Remote Hardware-Controller, der als Schnittstelle zur IPMI-fähigen Servermanagement-Hardware auf dem Dell-

Gerät dient. Dem DRAC ist eine IP-Adresse zugeordnet, die zur Identifizierung des DRAC bei der Erkennung und Verwaltung des Geräts dient.

Geräte mit Dell DRAC können mit den gleichen Funktionen verwaltet werden wie andere IPMI-fähige Geräte. Wenn das Gerät erkannt und zur Liste verwalteter Geräte hinzugefügt wurde, wird es genau wie alle anderen IPMI-Geräte gehandhabt. Außerdem verfügt System Manager über spezielle Dell DRAC-Funktionen.

Der OpenManage Server Administrator ist eine webbasierte Konsole von Dell zur Verwaltung des DRAC-Geräts. Normalerweise erfolgt der Zugriff durch Eingabe der IP-Adresse des DRAC in einen Browser und Anmeldung mit Benutzername und Kennwort. Wenn ein Dell DRAC-Gerät mit System Manager verwaltet wird, kann dieses Dienstprogramm auch direkt von der System Manager Schnittstelle aus gestartet werden.

Außerdem ermöglicht System Manager die Verwaltung von Benutzernamen und Kennwörtern für den Zugriff auf den OpenManager Server Administrator, und es werden drei Protokolle von diesem Dienstprogramm in der Serverinformationskonsole angezeigt.

So öffnen Sie den OpenManage Server Administrator für ein Dell DRAC-Gerät

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Erweitern Sie in der Serverinformationskonsole die Option **Hardware** und klicken Sie auf **Dell DRAC**. Die IP-Adresse sowie andere Informationen zur Identifizierung des Geräts werden angezeigt.
3. Klicken Sie auf **Dell DRAC Utility starten**, um den OpenManage Server Administrator des Geräts in einem neuen Fenster zu öffnen.

Dell DRAC-Protokolle befinden sich in System Manager.

Drei Protokolle vom OpenManage Server Administrator werden in der System Manager Serverinformationskonsole angezeigt.

- **Dell DRAC-Protokoll**: enthält alle vom Server Administrator aufgezeichneten Ereignisse, wie z. B. Anmeldeaktivität, Sitzungsstatus, Firmware-Update-Status sowie DRAC-Interaktion mit anderen Gerätekomponenten. In System Manager angezeigte Informationen sind u. a. Schwere des Fehlers, Beschreibung und empfohlene Fehlerbehebungsmaßnahmen.
- **Dell DRAC-Befehlsprotokoll**: enthält alle an den Server Administrator ausgegebenen Befehle. Es wird angegeben, welche Befehle wann und von wem ausgeführt wurden, einschließlich An- und Abmeldeversuche und Zugangsfehler.
- **Dell DRAC-Ablaufverfolgungsprotokoll**: hilfreich zur Ablaufverfolgung der Netzwerkkommunikation, z. B. Alarmierung, Paging oder Netzwerkverbindungen vom DRAC.

So sehen Sie die Protokolle für ein Dell DRAC-Gerät ein

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie in der Serverinformationskonsole auf **Protokolle**.
3. Klicken Sie auf **Dell DRAC-Protokoll**, **Dell DRAC-Befehlsprotokoll** oder **Dell DRAC-Ablaufverfolgungsprotokoll**.

Verwalten von Benutzernamen für Dell DRAC-fähige Geräte

Um auf die OpenManage Server Administrator-Schnittstelle zuzugreifen, melden Sie sich mit einem für das Gerät definierten Benutzernamen und Kennwort an. Der Standardbenutzer **root** erscheint als erster Benutzer in der Liste und kann nicht gelöscht werden. Das zugehörige Kennwort kann jedoch geändert werden. Es können bis zu 15 Benutzer hinzugefügt werden. DRAC-Benutzernamen können zwar verschiedene Zugangsebenen haben, System Manager definiert Benutzernamen jedoch nur auf der Administratorebene.

So können Sie Benutzernamen und Kennwörter für ein DRAC-fähiges Gerät hinzufügen oder bearbeiten

1. Doppelklicken Sie auf das Gerät in der Liste **Alle Geräte**.
2. Klicken Sie in der Serverinformationskonsole auf **Hardware-Konfiguration**.
3. Erweitern Sie in der Serverinformationskonsole die Option **Dell DRAC-Konfiguration** und klicken Sie auf **Dell DRAC-Benutzer**. Es wird eine Liste der derzeit definierten Benutzer angezeigt.
4. Um das Kennwort zu ändern, klicken Sie auf die Benutzernummer und dann auf **Kennwort ändern**. Nachdem Sie das neue Kennwort eingegeben und bestätigt haben, klicken Sie auf **Übernehmen**. (Um das gleiche Kennwort mehreren Benutzern zuzuweisen, wählen Sie dies mit Strg+Mausklick oder Umschalten+Mausklick aus.)
5. Um einen Benutzer hinzuzufügen, klicken Sie auf **Benutzer hinzufügen**. Geben Sie einen Benutzernamen und ein Kennwort ein, bestätigen Sie das Kennwort und klicken Sie auf **Übernehmen**. Der Benutzer wird zur Liste hinzugefügt.

   Hinweis: Wenn Sie einen Benutzernamen eingeben, der sich bereits in der Liste befindet, überschreibt das neue Kennwort, das Sie eingeben, das alte Kennwort für diesen Benutzernamen. Es wird kein zweiter Benutzer mit dem gleichen Namen zur Liste hinzugefügt.

6. Um einen Benutzer zu löschen, klicken Sie auf die Benutzernummer, auf **Benutzer löschen** und dann auf **OK**. (Um mehrere Benutzer zu löschen, wählen Sie diese mit Strg+Mausklick oder Umschalten+Mausklick aus.)

Alle Benutzer in dieser Liste haben Zugang auf der Administratorebene zum OpenManage Server Administrator.

Installation und Wartung der Core-Datenbank

Installation der Core-Datenbank

Die Standardinstallation für dieses Produkt installiert eine Microsoft MSDE-Datenbank auf dem Core Server. Dies ist die einzig verfügbare Datenbankoption für System Manager, und es kann nur eine Core-Datenbank installiert werden. Die Datenbank sollte ausschließlich auf einem Standalone-Server installiert werden.

Das Datenbankschema unterstützt Microsoft SQL Server 2000 mit SP4. Auf allen Datenbankservern muss MDAC 2.8 installiert sein.

Die auf Ihrem Core-Server installierte Datenbank muss eine komplett neue Datenbank sein. Wenn Sie System Manager auf einem Server installieren, auf dem zu einem früheren Zeitpunkt eine Installation von LANDesk® Management Suite oder Server Manager vorhanden war, können Sie die vorhandene Datenbankstruktur für Ihre Installation von System Manager nicht verwenden.

Das Programm LANDesk Dienste konfigurieren beinhaltet eine Benutzeroberfläche, über die Sie mehrere unterschiedliche Dienste konfigurieren können Die Registerkarte "Allgemein" zeigt den aktuellen Servernamen, Datenbanknamen und den Benutzernamen und das Kennwort an, der/das für den Zugriff auf die Core-Datenbank erforderlich ist. Die Berechtigungsnachweise werden von allen Diensten verwendet, die auf die Core-Datenbank zugreifen. Da System Manager nur eine Core-Datenbank verwenden kann, ist es nicht erforderlich, die Server- oder Datenbanknamen zu ändern. Falls erforderlich, können Sie die Berechtigungsnachweise ändern. Weitere Informationen finden Sie in Anhang A: Konfigurieren von Diensten.

Anhang A: Systemanforderungen und verwendete Anschlüsse

Der Core muss über eine statische IP-Adresse verfügen.

Administrativer Core

Der administrative Core unterstützt die folgenden Betriebssysteme:

- Microsoft Windows 2000 Server (mit SP4)
- Microsoft Windows 2000 Advanced Server (mit SP4)
- Microsoft Windows 2003 Server Standard Edition (mit SP1)
- Microsoft Windows 2003 Server Enterprise Edition (mit SP1)

Server-Support (Agents)

- Microsoft Windows 2000 Server (mit SP4)
- Microsoft Windows 2000 Advanced Server (mit SP4)
- Microsoft Windows 2000 Professional (mit SP4)
- Microsoft Windows 2003 Server Standard Edition x86 (mit SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (mit SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (mit SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (mit SP1)
- Microsoft Windows XP Professional (mit SP2)
- Microsoft Windows XP Professional x64 (mit SP2)
- Windows Small Business Server 2000 (mit SP4)
- Windows Small Business Server 2003 (mit SP1)
- Red Hat Enterprise Linux v3 (ES) 32-Bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-Bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-Bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32-Bit - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32-Bit - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32-Bit - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2

- SUSE* Linux Server 9 ES 32-Bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Browser

- Microsoft Internet Explorer 6.x (mit SP1)
- Mozilla, ab Version 1.7
- Firefox, ab Version 1.5

Datenbanken

- MSDE (mit SP4)

Microsoft Data Access-Komponenten

- MDAC, ab Version 2.8

Wenn mehr als ein LANDesk-Verwaltungsprodukt dieselbe Datenbank verwenden soll, müssen Sie beide Produkte auf demselben "Core"-Gerät installieren. Dementsprechend gilt, dass Sie dieselbe Datenbank verwenden müssen, wenn Sie mehrere Produkte auf demselben "Core"-Gerät installieren möchten. Wenn beide Produkte dieselbe Datenbank verwenden, dann müssen beide Produkte auch der Version 8.70 entsprechen.

Verwendete Anschlüsse

Einführung

Wenn Sie dieses Produkt in einer Umgebung verwenden, die Firewalls einschließt (oder Router, die den Datenverkehr filtern), müssen Sie möglicherweise Firewall- oder Router-Konfigurationen anpassen, um die Funktionsfähigkeit des Produkts zu gewährleisten. Dieser Abschnitt beschreibt die von den einzelnen Produktkomponenten verwendeten Anschlüsse. Die hier angegebenen Informationen beziehen sich vor allem auf die Konfiguration von Routern und Firewalls. Nur lokal (in den einzelnen Subnetzen) verwendete Anschlüsse werden nicht besprochen.

Hintergrundinformationen zu Firewall-Regeln

Diese Informationen gelten für das Einrichten von Firewall-Regeln. Falls Sie sich mit diesem Thema noch nicht auskennen, finden Sie in diesem Abschnitt allgemeine Hintergrundinformationen zu den wichtigsten Konzepten.

Firewall-Regeln

Einen "Anschluss öffnen" ist nicht so einfach wie es klingt. Sie können nicht einfach zu einer Firewall gehen und "Anschluss x öffnen". Einen Anschluss zu öffnen bedeutet eigentlich, eine Firewall-Regel zu erstellen. Firewall-Regeln beschreiben, welche Netzwerkdaten die Firewall passieren dürfen und welche nicht. Die Firewall-Regel filtert den Netzwerkverkehr nicht nur nach der Anschlussnummer. Regeln können auf Protokollen, Quell- und Zielanschlussnummern, Richtung (ankommend/abgehend), Quell- und Ziel-IP-Adressen usw. basieren.

Eine typische Firewall-Regel sieht so aus: "ankommenden Verkehr an TCP Anschluss 9535 zulassen". Für dieses Produkt wird diese Regel als Unterstützung für die Fernsteuerung benötigt. Die Regel basiert auf drei Elementen:

1. Dem Protokoll (TCP oder UDP)
2. Der Anschlussnummer
3. Der Richtung (ankommend oder abgehend)

Diese drei Elemente werden zum Einrichten von Firewall-Regeln benötigt.

Quell- und Zielanschlüsse, dynamische Anschlüsse

An der TCP- oder UDP-Kommunikation sind immer zwei Anschlüsse beteiligt. Alle TCP- oder UDP-Pakete gehen von einem Quellanschluss an einen Zielanschluss. Firewall-Regeln können auf dem Quellanschluss, dem Zielanschluss oder beiden basieren. Die in Dokumenten wie dem vorliegenden angegebenen Anschlüsse sind immer Zielanschlüsse.

Bekannte Anschlüsse wie 5007 (vom Inventardienst verwendet) beziehen sich nur auf eine Seite der Kommunikation. Für die andere Seite der Kommunikation wird ein dynamischer Anschluss verwendet. Dynamische Anschlüsse werden automatisch vom Betriebssystem im Bereich 1024 bis 5000 zugeordnet.

Firewalls und UDP-Verkehr

Um TCP-Verkehr durch eine Firewall (z. B. ankommende TCP-Verbindungen an Anschluss 5007) passieren zu lassen, genügt eine einzelne Regel. Sobald die TCP-Verbindung hergestellt ist, können Daten über diese Verbindung in beide Richtungen fließen.

Bei UDP-Verkehr ist das anders, da hier keine Verbindung besteht. Der Core Server unterzieht z. B. standardmäßig Geräte am UDP-Anschluss 38293 einem Ping-Test, bevor er einen Task startet. Eine Firewall-Regel, die abgehende UDP-Pakete an Anschluss 38293 zulässt, erlaubt ebenfalls Pakete vom Core Server an Geräte außerhalb der Firewall, jedoch nicht die Antwortpakete des jeweiligen Pakets.

Eine Regel, die sowohl abgehende als auch ankommende Pakete an Anschluss 38293 erlaubt, funktioniert ebenfalls nicht, da eine Seite der Kommunikation am bekannten Anschluss mithört. Die andere Seite verwendet einen dynamischen Anschluss. Da die vom Core Server abgehenden Pakete von einem dynamischen Anschluss an Anschluss 38293 gesendet werden, gehen die Antwortpakete des Geräts von Anschluss 38293 an den gleichen dynamischen Anschluss, nicht an Anschluss 38293. Um eine Kommunikation in beide Richtungen zu ermöglichen, ist eine

Regel nötig, die UDP-Pakete mit Anschluss 38293 als Quell- oder Zielanschluss zulässt. Eine solche Regel ist normalerweise akzeptabel für ein Intranet, nicht jedoch für eine externe Firewall (da sie ankommende Pakete an allen UDP-Anschlüssen erlauben würde).

Aus diesem Grund gilt UDP-Verkehr in der Regel nicht als Firewall-freundlich. Zurück zu unserem Beispiel: Es gibt eine Alternative zu UDP-Anschluss 38293, nämlich TCP-Anschluss 9595. Bei der Verwaltung Firewall-geschützter Geräte ist es daher vorzuziehen, das Produkt zur Verwendung des TCP-Anschluss zu konfigurieren.

Verwendete Anschlüsse

Anschluss	Richtung	Protokoll	Dienst
31770	Konsole nach Geräten, Gerät nach Core	TCP	Kommunikation zwischen Konsole und Gerät
9595, 9594	Konsole nach Gerät	TCP	Serverkonfiguration
9595	Konsole nach Gerät	UDP	Erkennung
623	Konsole nach Gerät	UDP	ASF, IPMI-Erkennung
5007	Konsole nach Gerät	TCP	Inventar
9535	Konsole nach Gerät	TCP	Fernsteuerung
139, 145	Konsole nach Gerät	TCP	Datei- und Druckerfreigabe
137, 138	Konsole nach Gerät	UDP	Datei- und Druckerfreigabe

Dieses Produkt muss Knoten erkennen, auf denen der Standard Management Agent installiert ist, damit er die Geräte verwalten kann. UDP Anschluss 9595 wird zur Erkennung verwendet. Sie können einzelne Geräte auch manuell der Konsole hinzufügen; dies setzt jedoch dennoch voraus, dass das Gerät einen "Ping" am UDP-Anschluss 9595 beantwortet. Die Kommunikation zwischen der Konsole und dem Gerät verwendet die TCP-Anschlüsse 31770 und 6787. Auf dem letzteren dieser beiden Anschlüsse ist der Verkehr HTTP-basiert. UDP-Anschluss 623 wird zur Erkennung von ASF (Alert Standard Forum) verwendet. Zusätzlich verwendet dieses Produkt TCP-Anschluss 9535 für die Fernsteuerung. Die IPMI-Erkennung ist mit der ASF-Erkennung verknüpft und verwendet den gleichen Anschluss (udp/623).

Anhang B: Aktivieren des Core Servers

Damit Sie die Konsole verwenden können, müssen Sie Ihren Core Server mit dem Core Server-Aktivierungsprogramm aktivieren. Im Allgemeinen muss diese Prozedur nur einmal durchgeführt werden; eine Wiederholung ist nur erforderlich, wenn Sie zusätzliche Lizenzen erwerben. Verwenden Sie das Core Server-Aktivierungsprogramm für folgende Aufgaben:

- Erste Aktivierung eines neuen Servers
- Aktualisieren eines vorhandenen Core Serversoder Upgrade auf Management Suite oder Server Manager.
- Aktivierung eines neuen Servers mit einer 45 Tage gültigen Probelizenz

Starten Sie das Programm, indem Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung** klicken. Wenn Ihr Core Server nicht an das Internet angeschlossen ist, lesen Sie die Informationen unter "Manuelles Aktivieren eines Core oder Überprüfen der Daten zur Knotenzahl" weiter unten in diesem Abschnitt.

Jeder Core Server benötigt ein eindeutiges Autorisierungszertifikat. Das Autorisierungszertifikat darf nicht von mehreren Core Servern gemeinsam benutzt werden; mehrere Core Server können jedoch Knotenzahlen beim selben LANDeskKonto verifizieren lassen. Dieses Dienstprogramm wird beim ersten Neustart nach der System Manager-Installation automatisch ausgeführt.

Der Core Server hinterlegt in regelmäßigen Abständen zu verifizierende Knotenzahldaten in der Datei "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Diese Datei wird in regelmäßigen Abständen an den LANDesk Software-Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den LANDesk Software-Lizenzserver ungültig.

Der Core kommuniziert mit dem LANDesk Software-Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte **Proxy** und geben die erforderlichen Proxy-Informationen ein. Wenn Ihr Core mit dem Internet verbunden ist, wird die Kommunikation mit dem Lizenzserver automatisch hergestellt, d.h., dass von Ihrer Seite keine manuellen Eingaben erforderlich sind. Wenn keine Verbindung mit dem Core besteht, klicken Sie beim Neustart auf **Schließen** und senden Sie die Autorisierungsdatei an licensing@landesk.com.

Das Core Server-Aktivierungsprogramm startet nicht automatisch eine DFÜ-Verbindung mit dem Internet. Wenn Sie jedoch die DFÜ-Verbindung manuell starten und das Aktivierungsprogramm ausführen, kann das Programm die DFÜ-Verbindung zum Übermitteln der Daten des Nutzungsberichts verwenden.

Wenn Ihr Core Server nicht mit dem Internet verbunden ist, können Sie Knotenzahldaten wie weiter unten beschrieben verifizieren und senden.

So aktivieren Sie einen Server mit einem LANDesk Software-Konto

Bevor Sie einen neuen Server mit einer Volllizenz aktivieren können, müssen Sie ein LANDesk Software-Konto einrichten, das Ihnen eine Lizenz für die von Ihnen erworbenen LANDesk Software-Produkte und Knoten erteilt. Sie benötigen die Kontoinformationen (Name der Kontaktperson und Kennwort), um Ihren Server zu aktivieren. Wenn Ihnen diese Informationen nicht vorliegen, wenden Sie sich an den zuständigen Vertriebsmitarbeiter bei LANDesk Software.

Ändern Sie nicht das Datum oder die Uhrzeit des Core Servers zwischen dem Installieren des Produkts und dem Aktivieren des Core. Diese Aktivierung wird misslingen. Sie müssen dann das Produkt deinstallieren und neu installieren.

So aktivieren Sie einen Server

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung**.
2. Klicken Sie auf **Aktivieren**.

Aktivieren eines Servers mit einer Probelizenz

Die 45 Tage gültige Probelizenz aktiviert Ihren Server auf dem LANDesk Software-Lizenzserver. Nach Ablauf der 45-tägigen Testzeit können Sie sich nicht mehr beim Core Server anmelden; der Core Server nimmt dann auch keine Inventarscans mehr entgegen. Ihre in der Software oder Datenbank vorhandenen Daten gehen jedoch nicht verloren. Während oder nach Verwendung der 45-tägigen Probelizenz können Sie das Core Server-Aktivierungstool erneut ausführen und Ihre Probelizenz in eine Vollaktivierung konvertieren, die mit einem LANDesk Software-Konto arbeitet. Wenn die Probelizenz abgelaufen ist, wird mit der Konvertierung in eine Volllizenz der Core reaktiviert.

So aktivieren Sie eine 45-tägige Probelizenz

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung**.
2. Klicken Sie auf **Aktivieren Sie diesen Core für eine 45-tägige Testzeit**.
3. Klicken Sie auf **Auswerten**.

Aktualisieren eines vorhandenen Kontos

Die Aktualisierungsoption sendet Nutzungsdaten an den LANDesk Software-Lizenzserver. Die Nutzungsdaten werden automatisch gesendet, wenn Ihr System über eine Internet-Verbindung verfügt. Es sollte sich daher im Allgemeinen für Sie nicht als notwendig erweisen, mit dieser Option Daten zur Verifizierung der Knotenzahl zu senden. Sie können mit dieser Option auch den mit dem LANDesk Software-Konto verbundenen Core Server ändern. Zudem können Sie mit dieser Option einen Core Server von einer Probelizenz in eine Volllizenz konvertieren.

So aktualisieren Sie ein vorhandenes Kontos

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung**.

2. Klicken Sie auf **Aktualisieren Sie diese Core Server mithilfe Ihres LANDesk-Kontaktnamens und -Kennworts**.
3. Geben Sie den Namen der **Kontaktperson** und das **Kennwort** ein, den/das der Core verwenden soll. Wenn Sie einen Namen oder ein Kennwort eingeben, das sich von dem für die ursprüngliche Aktivierung des Core Servers verwendeten Namen oder Kennwort unterscheidet, wird der Core hiermit dem neuen Konto zugeordnet.
4. Klicken Sie auf **Aktivieren**.

Manuelles Aktivieren eines Core oder Überprüfen der Knotenzahldaten

Wenn der Core Server nicht mit dem Internet verbunden ist, kann das Core Server-Aktivierungsprogramm keine Informationen bzgl. der Knotenzahl senden. In diesem Fall erhalten Sie eine Meldung, in der Sie aufgefordert werden, Verifizierungsdaten zur Aktivierung und zur Knotenzahl manuell per E-Mail zu senden. Die E-Mail-Aktivierung ist ein schnelles und unkompliziertes Verfahren. Wenn die Aufforderung zur manuellen Aktivierung auf dem Core angezeigt wird, oder wenn Sie das Core Server-Aktivierungsprogramm verwenden und die manuelle Aktivierungsmeldung angezeigt wird, führen Sie folgende Schritte aus:

So aktivieren Sie einen Core manuell oder veranlassen eine manuelle Überprüfung der Knotenzahldaten

1. Wenn der Core Sie auffordert, die Daten zur Knotenzahl manuell zu verifizieren, erstellt er eine Datendatei mit dem Namen ACTIVATE.TXT im Ordner \Program Files\LANDesk\Authorization Files. Fügen Sie diese Datei einer E-Mail-Nachricht bei und senden Sie sie an licensing@landesk.com. Betreff und Nachrichtentext können frei gewählt werden.
2. LANDesk Software verarbeitet die beigefügte Datei und schickt eine Antwort an die E-Mail-Adresse, von der aus Sie die Nachricht gesendet hatten. Die LANDesk Software-Nachricht enthält Instruktionen und eine neue Autorisierungsdatei.
3. Öffnen Sie die beigefügte Autorisierungsdatei im Ordner \Program Files\LANDesk\Authorization Files. Die Datei wird daraufhin sofort vom Core Server verarbeitet und ihr Aktivierungsstatus aktualisiert.

Wenn die manuelle Aktivierung misslingt oder der Core die beigefügte Aktivierungsdatei nicht verarbeiten kann, wird die von Ihnen kopierte Autorisierungsdatei unter Verwendung der Erweiterung ".rejected" umbenannt. Zusätzlich hierzu protokolliert das Aktivierungsprogramm unter Angabe weiterer Details ein Ereignis im Anwendungsprotokoll der Windows-Ereignisanzeige.

Anhang C: Konfigurieren von Diensten

Mit dem Applet "Dienste konfigurieren" können Sie folgende Dienste für Ihre Core Server und Datenbanken konfigurieren:

- Auswählen eines Core Servers und einer Datenbank
- Konfigurieren des Inventardienstes
- Konfigurieren des Vorgehens bei doppelten Gerätenamen
- Konfigurieren des Vorgehens bei doppelten Gerätekennungen
- Konfigurieren des Scheduler-Dienstes
- Konfigurieren des benutzerdefinierten Auftragsdienstes
- Konfigurieren des Multicast-Dienstes
- Konfigurieren des BMC-Kennworts
- Konfigurieren des Intel AMT-Kennworts

Um das Applet "Dienste konfigurieren" auf dem Core Server zu starten, klicken Sie auf **Start | Programme | LANDesk | LANDesk Dienste konfigurieren**.

Zwei Schaltflächen werden außerhalb der Registerkarten angezeigt:

- **Berechtigungsnachweise:** Öffnet das Dialogfeld "Serverberechtigungsnachweise". In diesem Dialogfeld können Sie Geräte hinzufügen, die als bevorzugte Server fungieren können. Klicken Sie auf **Hinzufügen**, um ein Gerät hinzuzufügen. Hiermit wird das Dialogfeld **Benutzername und Kennwort** (siehe Beschreibung weiter unten) geöffnet.
- **OSD-Validierung:** Um Windows PE- oder DOS-basierte Preboot-Umgebungen erstellen zu können, müssen Sie Zugriff auf die Windows PE 2005- und Windows NT 4-Installations-CDs bereitstellen. Klicken Sie unter beiden Abbilderstellungsumgebungen auf **Jetzt verifizieren**, geben Sie den Pfad zur korrekten CD ein und klicken Sie auf **OK**.

Dialogfeld "Benutzername und Kennwort"

Verwenden Sie das Dialogfeld **Benutzername und Kennwort**, um Informationen zu bevorzugten Servern, die Sie hinzufügen möchten, bereitzustellen.

So geben Sie Informationen zu bevorzugten Servern ein

1. Klicken Sie im Applet "Dienste konfigurieren" auf **Berechtigungsnachweise**.
2. Klicken Sie im Dialogfeld "Serverberechtigungsnachweise" auf **Hinzufügen**.
3. Geben Sie eine Beschreibung, Authentifizierungsdaten und IP-Adressbereiche ein.
4. Klicken Sie auf **Berechtigungsnachweise testen**, um die Gültigkeit Ihrer Informationen zu überprüfen.
5. Klicken Sie auf **OK**, um den bevorzugten Server dem Dialogfeld "Serverberechtigungsnachweise" hinzuzufügen.

- **Servername:** Der Name des bevorzugten Servers.
- **Benutzername:** Der Benutzername für die Authentifizierung gegenüber dem Server. Es muss ein vollständig qualifizierter Domänenname sein (z. B. Mydomain\user name).
- **Beschreibung:** Eine Beschreibung des bevorzugten Servers.
- **Kennwort:** Das Kennwort des bevorzugten Servers.

- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressbereich ein, auf den Sie die Verwendung des bevorzugten Servers beschränken möchten. Die Start-IP-Adresse darf nicht größer sein als die Abschluss-IP-Adresse. Die ersten drei Oktette der Start- und Abschluss-IP-Adressen müssen übereinstimmen, z. B. 10.100.10.1 und 10.100.10.255.
- **Letzte IP-Adresse:** Geben Sie die Abschluss-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Hinzufügen:**Fügt den IP-Adressbereich in die Warteschlange im unteren Abschnitt des Dialogfelds ein.
- **Löschen:** Entfernt den ausgewählten IP-Adressbereich aus der Arbeitswarteschlange.

Konfigurieren der Registerkarten für Dienste

Geben Sie vor dem Konfigurieren des Dienstes auf der Registerkarte **Allgemein** den Core Server und die Datenbank an, für die Sie den Dienst konfigurieren möchten.

Hinweis: Wenn Sie die Konfiguration eines Dienstes für einen Core Server und eine Datenbank ändern, werden diese Änderungen erst übernommen, wenn Sie den Dienst auf dem betreffenden Core Server neu starten.

Auswählen eines Core Servers und einer Datenbank

Auf der Registerkarte **Allgemein** können Sie einen Core Server und eine Datenbank auswählen und Authentifizierungsnachweise bereitstellen, sodass Sie Dienste für den Core Server konfigurieren können.

Informationen zum Dialogfeld "Alarme konfigurieren": Registerkarte "Allgemein"

Wählen Sie in diesem Dialogfeld den Core Server und die Datenbank aus, für die Sie einen bestimmten Dienst konfigurieren möchten. Wählen Sie dann die Registerkarte "Dienst" aus und definieren Sie die Einstellungen für diesen Dienst.

- **Servername:** Zeigt den Namen des Core Servers an, mit dem Sie gegenwärtig verbunden sind.
- **Server:** Hier können Sie den Namen eines anderen Core Servers und dessen Datenbankverzeichnis eingeben.
- **Datenbank:** Hier können Sie den Namen der Core-Datenbank eingeben.
- **Benutzername:** Identifiziert einen Benutzer mit Berechtigungsnachweisen gegenüber der Core-Datenbank (während des Setup festgelegt).
- **Kennwort:** Identifiziert das Benutzerkennwort, das für den Zugriff auf die Core-Datenbank erforderlich ist (während des Setup festgelegt).
- **Dies ist eine Oracle-Datenbank:** gibt an, dass die oben festgelegte Datenbank eine Oracle-Datenbank ist. (Gilt nicht für System Manager.)
- **Einstellungen aktualisieren:** stellt die vorhandenen Einstellungen wieder her, wenn Sie das Dialogfeld "Dienstkonfiguration" geöffnet haben.

Konfigurieren des Inventardienstes

Konfigurieren Sie auf der Registerkarte **Inventar** den Inventardienst für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Informationen zum Dialogfeld "Dienste konfigurieren": Registerkarte "Inventar"

Definieren Sie mithilfe dieser Registerkarte die folgenden Inventaroptionen:

- **Servername**: Zeigt den Namen des Core Servers an, mit dem Sie gegenwärtig verbunden sind.
- **Statistik protokollieren:** Legt ein Protokoll mit den Aktionen der Core-Datenbank und mit Statistiken an.
- **Verschlüsselter Datentransport:** Ermöglicht es dem Inventarscanner, Daten zum Geräteinventar als verschlüsselte Daten über SSL zurück an den Core Server zu senden.
- **Server inventarisieren um**: Gibt die Uhrzeit für die Durchführung des Core Server-Scans an.
- **Wartung durchführen um:** Gibt die Uhrzeit für die Standardwartung der Core-Datenbank an.
- **Tage, die Inventarscans gespeichert bleiben:** Legt fest, nach wie vielen Tagen die Daten des Inventarscans gelöscht werden.
- **Anmeldedaten des primären Eigentümers**: Legt fest, wie oft der Inventarscanner Anmeldungen verfolgt, um den primären Eigentümer eines Geräts zu bestimmen. Der primäre Eigentümer ist der Benutzer, der sich innerhalb dieser vorgegebenen Anzahl von Anmeldungen am häufigsten angemeldet hat. Der Standardwert ist 5 und Mindest- bzw. Höchstwerte sind 1 bzw. 16. Wenn alle Anmeldenamen unterschiedlich sind, wird der letzte Benutzer, der sich anmeldet, als primärer Eigentümer betrachtet. Ein Gerät kann nur jeweils mit einem primären Eigentümer verknüpft sein. Die Anmeldedaten des primären Eigentümers beinhalten den voll qualifizierten Namen des Benutzers entweder im ADS-, NDS-, Domänennamen- oder im lokalen Namensformat (in dieser Reihenfolge) und das Datum der letzten Anmeldung.
- **Erweiterte Einstellungen:** Öffnet das Dialogfeld **Erweiterte Einstellungen**. In diesem Dialogfeld können Sie zahlreiche Zusatzeinstellungen für den Inventarscanner festlegen. Klicken Sie auf die Einstellung, ändern Sie die Einstellung im Textfeld **Wert** und klicken Sie dann auf **Festlegen**, um eine Einstellung zu ändern. Um eine Beschreibung einer Einstellung anzuzeigen, klicken Sie auf die Einstellung und zeigen Sie die Details im Feld **Beschreibung** an.
- **Software:** Öffnet das Dialogfeld **Softwarescaneinstellungen**, in dem Sie die Scanzeit der Serversoftware und die Verlaufseinstellungen konfigurieren können.
- **Attribute:** Öffnet das Dialogfeld "Attribute zu speichern auswählen", in dem Sie die in der Datenbank zu speichernden Inventarscanattribute auswählen können.
- **Duplikate verwalten: Geräte**: Öffnet das Dialogfeld Handhabung von Duplikaten. In diesem Dialogfeld können Sie eine Option zum Entfernen von Geräten mit doppelt vorhandenen Gerätenamen, MAC-Adressen oder beidem auswählen (siehe **Doppelt vorhandene Geräte** weiter unten).

- **Duplikate verwalten: Geräte-IDs:**Öffnet das Dialogfeld **Doppelte Gerätekennung**. In diesem Dialogfeld können Sie Attribute auswählen, mit denen sich Geräte eindeutig identifizieren lassen. Sie können mit dieser Option verhindern, dass doppelte Gerätekennungen in die Core-Datenbank gescannt werden (siehe Konfigurieren des Vorgehens bei doppelten Gerätekennungen weiter unten).
- **Status Inventardienst:** Zeigt an, ob der Dienst auf dem Core Server gestartet oder angehalten wurde.
- **Start**: Startet den Dienst auf dem Core Server.
- **Stopp**: Stoppt den Dienst auf dem Core Server.

Informationen zum Dialogfeld "Softwarescaneinstellungen"

In diesem Dialogfeld können Sie die Häufigkeit von Softwarescans konfigurieren. Die Hardware eines Geräts wird jedes Mal gescannt, wenn der Inventarscanner auf dem Gerät ausgeführt wird; die Software eines Geräts wird jedoch nur in den von Ihnen hier angegebenen Abständen gescannt.

- **Bei jeder Anmeldung:** Prüft bei jeder Anmeldung des Benutzers die gesamte Software, die auf dem Gerät installiert ist.
- **Mindestens Abstand (Tage)::** Prüft die auf dem Gerät installierte Software nur in dem angegebenen Tagesintervall (automatischer Scan).
- **Verlauf speichern (Tage):** Gibt an, wie lange der Inventarverlauf des Geräts gespeichert bleibt.

Konfigurieren des Vorgehens bei doppelten Gerätenamen

Verwenden Sie das Dialogfeld "Doppelte Geräte", um doppelt vorhandene Geräte aus der Datenbank zu löschen.

1. Klicken Sie auf der Registerkarte "Inventar" auf **Geräte**.
2. Klicken Sie im Dialogfeld "Doppelte Geräte" auf die Option, die Sie beim Löschen doppelt vorhandener Geräte verwenden möchten, und klicken Sie dann auf **OK**.

   Doppelte Kennungen entfernen wenn:
   - **Gerätenamen übereinstimmen:** Entfernt den älteren Datensatz, wenn zwei oder mehr Gerätenamen in der Datenbank identisch sind.
   - **MAC-Adressen übereinstimmen:** Entfernt den älteren Datensatz, wenn zwei oder mehr MAC-Adressen in der Datenbank identisch sind.
   - **Gerätenamen und MAC-Adressen übereinstimmen:** Entfernt den älteren Datensatz NUR, wenn zwei oder mehr Gerätenamen und MAC-Adressen (für denselben Datensatz) identisch sind.

Konfigurieren des Vorgehens bei doppelten Gerätekennungen

Da in einem Netzwerkbetrieb zum Konfigurieren von Geräten häufig Abbilder verwendet werden, häuft sich das Risiko, dass unter den Geräten doppelte Gerätekennungen vorliegen. Sie können

dieses Problem vermeiden, indem Sie andere Geräteattribute spezifizieren, die in Kombination mit der Geräte-ID in der Lage sind, Ihre Geräte eindeutig zu kennzeichnen. Zu diesen anderen Attributen gehören beispielsweise Gerätename, Domänenname, BIOS, Bus, Koprozessor usw.

Mit der Funktion "Doppelte Kennung" können Sie Geräteattribute auswählen, die zur eindeutigen Kennzeichnung des Servers verwendet werden können. Sie geben an, um welche Attribute es sich handelt und wie viele von diesen Attributen identisch sein müssen, damit das Gerät als das Duplikat eines anderen Geräts ausgewiesen wird. Wenn der Inventarscanner ein identisches Gerät erkennt, schreibt er ein Ereignis in das Ereignisprotokoll der Anwendung, um auf die Geräte-ID des identischen Geräts zu verweisen. Das Dialogfeld "Doppelte Gerätekennung" enthält folgende Optionen:

- **Attributsliste:** Führt alle Attribute auf, die Sie auswählen können, um ein Gerät eindeutig zu kennzeichnen.
- **Identitätsattribute:** Zeigt die Attribute an, die Sie ausgewählt haben, um ein Gerät eindeutig zu kennzeichnen.
- **Doppelte Geräte-ID – Auslöser:**
    - **Identitätsattribute:** Bezeichnet die Anzahl Attribute, für die ein Gerät Übereinstimmungen melden muss, damit es als Duplikat eines anderen Geräts ausgewiesen wird.
    - **Hardware-Attribute:** Bezeichnet die Anzahl Hardwareattribute, für die ein Gerät fehlende Übereinstimmung melden muss, bevor es als Duplikat eines anderen Geräts ausgewiesen wird.
- **Doppelte Kennungen ablehnen:** Veranlasst den Inventarscanner, die Geräte-ID des Duplikat-Geräts aufzuzeichnen und alle nachfolgenden Versuche, diese Geräte-ID zu scannen, abzulehnen. Der Inventarscanner generiert daraufhin eine neue Geräte-ID.

So konfigurieren Sie die Behandlung von doppelten Kennungen

1. Klicken Sie im Dialogfeld "Dienste konfigurieren" auf die Registerkarte **Inventar** und dann auf **Geräte-ID**.
2. Wählen Sie aus der **Attributsliste** die Attribute aus, die Sie verwenden möchten, um ein Gerät eindeutig zu kennzeichnen, und klicken Sie dann auf den nach rechts zeigenden Pfeil, um das Attribut zur Liste **Identitätsattribute** hinzuzufügen. Sie können beliebig viele Attribute hinzufügen.
3. Wählen Sie die Anzahl der Identitätsattribute (und Hardwareattribute) aus, für die ein Gerät fehlende Übereinstimmung melden muss, bevor es als Duplikat eines anderen Geräts ausgewiesen wird.
4. Wenn Sie möchten, dass doppelte Gerätekennungen zurückgewiesen werden, aktivieren Sie die Option **Doppelte Kennungen ablehnen**.

Konfigurieren des Scheduler-Dienstes

Verwenden Sie die Registerkarte **Scheduler**, um den Scheduler-Dienst für den Core Server und für die Datenbank zu konfigurieren, den/die Sie mithilfe der Registerkarte **Allgemein** ausgewählt haben. Sie müssen über die erforderlichen Rechten für die Ausführung dieser Aufgaben verfügen, einschließlich aller Administratorrechte für die verwalteten Geräte, um den Empfang von Paketverteilungen von System Manager zu ermöglichen. Sie können mehrere auf den Geräten zu verwendende Berechtigungsnachweise für die Anmeldung angeben, indem Sie auf **Anmeldung ändern** klicken.

Informationen zum Dialogfeld "Dienste konfigurieren": Registerkarte "Scheduler"

Mithilfe dieser Registerkarte können Sie den Namen des Core Servers und der Datenbank anzeigen, die Sie zuvor ausgewählt haben, und die folgenden Optionen für einen geplanten Task festlegen:

- **Benutzername**: Der Benutzername, unter dem der Dienst "Geplante Tasks" ausgeführt wird. Er kann durch Klicken auf die Schaltfläche **Anmeldung ändern** geändert werden.
- **Anzahl Sek. zw. Wiederholungsversuchen:** Wenn eine geplante Task mit mehreren Wiederholungen konfiguriert ist, steuert diese Einstellung die Anzahl der Sekunden, die vor einer Wiederholung der Task vergehen müssen.
- **Anzahl Sek. für Reaktivierungsversuche:** Wenn ein geplanter Task mit Wake On LAN konfiguriert wurde, wird mit dieser Einstellung festgelegt, wie viele Sekunden der Dienst "Geplante Tasks" wartet, bevor er ein Gerät reaktiviert.
- **Intervall zwischen Abfrageevaluierungen:** Eine Zahl, die die Zeitspanne zwischen Abfrageauswertungen angibt, und eine Maßeinheit für die Zahl (Minuten, Stunden, Tage oder Wochen).
- **Wake on LAN-Einstellungen**: Der **IP-Anschluss**, der der von dem Wake On LAN*-Paket verwendet wird, das von den geplanten Tasks zum Reaktivieren von Geräten festgelegt wurde.
- **Status des Planungsdienstes**: Zeigt an, ob der Dienst auf dem Core Server gestartet oder angehalten wurde.
- **Start**: Startet den Dienst auf dem Core Server.
- **Stopp**: Stoppt den Dienst auf dem Core Server.
- **Neustart:** Startet den Dienst auf dem Core Server neu.
- **Erweitert:** Öffnet das Dialogfeld **Erweiterte Scheduler-Einstellungen**, in dem Sie die Einstellungen für die Arbeitsweise des Schedulers ändern können. Klicken Sie auf **Bearbeiten**, ändern Sie die Einstellung und klicken Sie auf **OK**, um eine Einstellung zu ändern.

Informationen zum Dialogfeld "Alarme konfigurieren": Dialogfeld "Anmeldung ändern"

Verwenden Sie das Dialogfeld **Anmeldung ändern** (klicken Sie auf **Anmeldung ändern** in der Registerkarte **Scheduler**), um die Standardanmeldung für den Scheduler zu ändern. Sie können zudem auch alternative Berechtigungsnachweise konfigurieren, die vom Scheduler-Dienst eingegeben werden sollten, wenn dieser einen Task auf nicht verwalteten Geräten ausführen muss.

Um System Manager-Agenten auf nicht verwalteten Geräten zu installieren, muss der Scheduler-Dienst in der Lage sein, mit einem administrativen Konto Verbindungen zu Geräten herzustellen. LocalSystem ist das vom Scheduler-Dienst verwendete Standardkonto. Die LocalSystem-Berechtigungsnachweise funktionieren im Allgemeinen für Geräte, die sich nicht in der Domäne befinden. Bei Geräten, die sich in einer Domäne befinden, müssen Sie ein Domänenadministrator-Konto angeben.

Wenn Sie die Berechtigungsnachweise für die Anmeldung des Scheduler-Dienstes ändern möchten, können Sie ein anderes Domänenebene-Verwaltungskonto zur Verwendung auf

Geräten angeben. Wenn Sie Geräte über mehrere Domänen hinweg verwalten, können Sie zusätzliche Berechtigungsnachweise hinzufügen, die der Scheduler-Dienst verwenden kann. Wenn Sie anstatt des LocalSystem-Kontos ein anderes Konto für den Scheduler-Dienst verwenden oder alternative Berechtigungsnachweise anbieten möchten, müssen Sie eine primäre Scheduler-Dienst-Anmeldung angeben, die über Core Server-Administratorrechte verfügt. Alternative Berechtigungsnachweise benötigen keine Core Server-Administratorrechte, müssen jedoch Administratorrechte auf Geräten besitzen.

Der Scheduler-Dienst versucht zunächst, sich mit den Standard-Berechtigungsnachweise anzumelden. Wenn dies nicht gelingt, wiederholt er den Vorgang so lange mit jedem einzelnen Berechtigungsnachweis, den Sie in der Liste **Alternative Berechtigungsnachweise** angegeben haben, bis keine Berechtigungsnachweise mehr vorhanden sind, mit denen er versuchen könnte, sich anzumelden. Von Ihnen angegebene Berechtigungsnachweise werden verschlüsselt und in der Registrierung des Core Servers gespeichert.

Sie können die folgenden Optionen für die Standard-Scheduler-Berechtigungsnachweise festlegen:

- **Benutzername:** Geben Sie den Standarddomänennamen\Standardbenutzernamen oder den Benutzernamen ein, den der Scheduler verwenden soll.
- **Kennwort:** Geben Sie das Kennwort für die von Ihnen festgelegten Berechtigungsnachweise ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Sie können die folgenden Optionen für zusätzliche Scheduler-Berechtigungsnachweise festlegen:

- **Hinzufügen:** Klicken Sie, um den Benutzernahmen und das Kennwort hinzuzufügen, das Sie in der Liste "Alternativen-Authentifizierung" angegeben haben.
- **Entfernen:** Klicken Sie, um die ausgewählten Berechtigungsnachweise aus der Liste zu entfernen.
- **Ändern:** Klicken Sie, um die ausgewählten Berechtigungsnachweise zu ändern.

Geben Sie beim Hinzufügen alternativer Berechtigungsnachweise Folgendes an:

- **Benutzername:** Geben Sie den Benutzernamen ein, den der Scheduler verwenden soll.
- **Domäne:** Geben Sie die Domäne für den von Ihnen angegebenen Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort für die von Ihnen festgelegten Berechtigungsnachweise ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Konfigurieren des Dienstes für benutzerdefinierte Aufträge

Konfigurieren Sie mithilfe der Registerkarte **Benutzerdefinierte Aufträge** den Dienst für benutzerdefinierte Aufträge für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben. Zu den benutzerdefinierten Aufträgen gehören beispielsweise Inventarscans oder Softwareverteilungen.

Wenn Sie die TCP-Fernausführung als Fernausführungsprotokoll deaktivieren, verwendet die Option "Benutzerdefinierte Aufträge" standardmäßig das Protokoll des Standard Management

Agent, unabhängig davon, ob es deaktiviert ist oder nicht. Wenn sowohl die TCP-Fernausführung als auch Standard Management Agent aktiviert sind, versucht die Option "Benutzerdefinierte Aufträge" zuerst, die TCP-Fernausführung zu verwenden. Wenn diese nicht vorhanden ist, wird die Standard-Fernausführung des Produkts verwendet.

Auf der Registerkarte **Benutzerdefinierte Aufträge** können Sie Optionen für die Erkennung von Servern auswählen. Damit die benutzerdefinierte Auftragsverarbeitung einen Auftrag bearbeiten kann, muss sie die aktuelle IP-Adresse des Servers ausfindig machen. Mit dieser Registerkarte können Sie festlegen, wie der Dienst mit den Servern Kontakt aufnimmt.

Informationen zum Dialogfeld "Dienste konfigurieren": Registerkarte "Benutzerdefinierte Tasks"

Definieren Sie mithilfe dieser Registerkarte die folgenden Optionen für benutzerdefinierte Aufträge:

Fernausführungsoptionen:

- **TCP-Ausführung deaktivieren**: Deaktiviert TCP als Fernausführungsprotokoll und verwendet standardmäßig das CBA-Protokoll.
- **CBA-Ausführung/Dateitransfer deaktivieren:** Deaktivert den Standard Management Agent als das Fernausführungsprotokoll. Wenn der Standard Management Agent deaktiviert ist und das TCP-Fernausführungsprotokoll nicht auf dem Gerät gefunden wird, misslingt die Fernausführung.
- **Timeout f. Fernausführung aktivieren:** Aktiviert ein Fernausführungs-Timeout und legt fest, nach wie vielen Sekunden das Timeout erfolgt. Fernausführungs-Timeouts werden ausgelöst, wenn das Gerät Heartbeat-Signale sendet, der Auftrag auf dem Gerät jedoch hängen geblieben ist oder sich in einer Schleife befindet. Diese Einstellung wird auf beide Protokolle angewendet (TCP und Standard Management Agent). Dieser Wert kann zwischen 300 Sekunden (5 Minuten) und 86400 Sekunden (1 Tag) liegen.
- **Client-Timeout aktivieren**: Aktiviert ein Geräte-Timeout und legt fest, nach wie vielen Sekunden das Timeout stattfindet. Standardmäßig sendet die TCP-Fernausführung ein Heartbeat-Signal vom Gerät an das Gerät in Intervallen von 45 Sekunden, bis die Fernausführung abgeschlossen ist oder ein Timeout erfolgt. Client-Timeouts werden ausgelöst, wenn das Gerät kein Heartbeat-Signal an das Gerät sendet.
- **Fernausführungsport (Standard 12174):** Der Anschluss, über den die TCP-Fernausführung erfolgt. Wenn dieser Anschluss geändert wird, muss er auch in der Clientkonfiguration geändert werden.

Verteilungsoptionen:

- **Verteilen an <nn> Server gleichzeitig**: Die maximale Anzahl Geräte, an die benutzerdefinierte Aufträge gleichzeitig verteilt werden.

Erkennungsoptionen:

- **UDP:** Wenn Sie UDP auswählen, wird ein Standard Management Agent-Ping über UDP verwendet. Die meisten System Manager-Komponenten setzen den Standard Management Agent voraus. Aus diesem Grund sollte auf Ihren verwalteten Geräten der Standard Management Agent installiert sein. Dies ist die schnellste Erkennungsmethode und gleichzeitig der Standard. Mit UDP können Sie auch die **Wiederholungen** und das **Timeout** für den UDP-Ping auswählen.
- **TCP:** Wenn Sie TCP auswählen, wird eine HTTP-Verbindung mit dem Server auf Anschluss 9595 benutzt. Diese Erkennungsmethode hat den Vorteil, dass sie über eine Firewall hinweg einsatzfähig ist, wenn Sie Port 9595 öffnen; die Methode unterliegt jedoch HTTP-Verbindungs-Timeouts, wenn keine Geräte vorhanden sind. Diese Timeouts können 20 Sekunden oder länger beanspruchen. Wenn eine große Zahl von Zielgeräten nicht auf die TCP-Verbindung reagiert, dauert es einige Zeit, bis Ihr Auftrag gestartet werden kann.
- **Beides:** Wenn Sie "Beide" auswählen, versucht der Dienst die Erkennung erst mit UDP, dann mit TCP und zuletzt mit DNS/WINS (sofern ausgewählt) durchzuführen.
- **Subnetz-Broadcast deaktivieren:** Wenn Sie diese Option auswählen, wird die Erkennung über ein Subnetz-Broadcast deaktiviert.
- **DNS/WINS-Lookup deaktivieren:** Wenn diese Option ausgewählt ist, deaktiviert sie einen Name Service Lookup für jedes Gerät, wenn die ausgewählte TCP/UDP-Erkennungsmethode scheitert.

Konfigurieren des Multicast-Dienstes

Konfigurieren Sie auf der Registerkarte **Multicast** die Erkennungsoptionen für Multicast-Domänenrepräsentanten für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte **Allgemein** ausgewählt haben.

Informationen zum Dialogfeld "Dienste konfigurieren": Registerkarte "Multicast"

Definieren Sie mithilfe dieser Registerkarte die folgenden Multicast-Optionen:

- **Multicast-Domänenrepräsentanten:** Verwendet die Liste mit den Multicast-Domänenrepräsentanten, die in der Gruppe **Konfiguration > Multicast-Domänenrepräsentanten** der Netzwerkansicht enthalten ist.
- **Cachedatei verwenden:** Fragt jede Multicast-Domäne ab, um herauszufinden, wo die Datei bereits in Cache gespeichert ist. Auf diese Weise lässt sich die im Cache gespeicherte Datei verwenden, anstatt die Datei in einen Vertreter herunterzuladen.
- **Cachedatei vorbevorzugtem Domänenrepräsentanten verwenden:**Ändert die Reihenfolge der Erkennung, sodass **Cachedatei verwenden** die erste Option ist, die das System auszuführen versucht.
- **Broadcast verwenden:** Sendet einen Subnetz-Broadcast, um alle Geräte in dem betreffenden Subnetz zu finden, die Multicast-Domänenrepräsentanten sein könnten.
- **Protokoll-Verwerfungszeitraum (Tage): Legt die** Anzahl der Tage fest, die Einträge im Protokoll bis zum Löschen erhalten bleiben.

Konfigurieren des BMC-Kennworts

Verwenden Sie die Registerkarte **BMC-Kennwort**, um ein Kennwort für den IPMI Baseboard Management Controller (BMC) zu erstellen.

- Geben Sie auf der Registerkarte **BMC-Kennwort** ein Kennwort in das Textfeld **Kennwort** ein, geben Sie das Kennwort erneut in das Textfeld **Kennwort bestätigen** ein und klicken Sie dann auf **OK**.

  Das Kennwort darf maximal 15 Zeichen beinhalten, wovon jedes Zeichen entweder eine Zahl von 0 - 9 oder ein Groß-/Kleinbuchstaben (a-z) sein muss.

Konfigurieren von Intel AMT-Optionen

Verwenden Sie die Registerkarte **Intel AMT-Konfiguration**, um das Kennwort auf Intel Active Management Technology-tauglichen Geräten zu erstellen oder zu ändern und Anweisungen zur Erkennung von AMT-Geräten anzuzeigen.

So konfigurieren Sie ein Intel AMT-Kennwort

1. Geben Sie den aktuellen Benutzernamen und das aktuelle Kennwort ein. Diese müssen mit dem Benutzernamen und dem Kennwort übereinstimmen, die auf dem Intel AMT-Konfigurationsbildschirm konfiguriert wurden (auf diesen Bildschirm wird über die BIOS-Einstellungen des Computers zugegriffen).
2. Um den Benutzernamen und das Kennwort zu ändern, füllen Sie den Abschnitt **Neues Intel AMT-Kennwort** aus.
3. Klicken Sie auf **OK**. Diese Änderung wird vorgenommen, wenn die Clientkonfiguration ausgeführt wird.

Hinweis: Das neue Kennwort muss ein starkes Kennwort sein, damit ist Folgendes gemeint:

- Es muss mindestens sieben Zeichen beinhalten
- Es muss Buchstaben, Zahlen und Symbole beinhalten
- Es besitzt mindestens ein Symbolzeichen in der zweiten bis zur sechsten Position
- Es unterscheidet sich deutlich von früheren Kennwörtern
- Es enthält keine Namen oder Benutzernamen
- Es handelt sich nicht um ein Gebrauchswort oder einen Namen

Erkennen und Versorgen von Intel AMT-Geräten

Geben Sie für die Erkennung von AMT-Geräten die IP-Adresse des Core Servers in das Feld "Provisioning Server" des AMT BIOS ein. Verwenden Sie Anschluss 9982. Klicken Sie unter **Dienste konfigurieren** auf **Hilfe** in , um weitere Informationen zu erhalten. Ein Intel AMT-Gerät, das erkannt und in die Liste **Eigene Geräte** verschoben wird, wird automatisch unter Verwendung des Modus bereitgestellt.

Anhang D: Agentensicherheit und vertrauenswürdige Zertifikate

Jeder Core Server verfügt über ein eindeutiges Zertifikat und einen privaten Schlüssel. Diese beiden Komponenten werden vom Setup erstellt, wenn Sie den Core Server erstmalig auf einem Gerät installieren. Geräte kommunizieren nur mit Core Servern, für die sie eine entsprechende vertrauenswürdige Zertifikatsdatei besitzen.

Die folgenden privaten Schlüssel- und Zertifikatsdateien werden installiert:

- **<Schlüsselname>.key:** Die .KEY-Datei ist der private Schlüssel für den Core Server; sie ist nur auf dem Core Server resident. Wenn dieser Schlüssel gefährdet ist, sind Core Server und Serverkommunikation nicht mehr sicher. Achten Sie auf die Sicherheit dieses Schlüssels. Senden Sie ihn beispielsweise nicht per E-Mail.
- **<Schlüsselname>.crt:** Die .CRT-Datei enthält den öffentlichen Schlüssel für den Core Server. Die .CRT-Datei ist eine Version des öffentlichen Schlüssels, die sich leichter anzeigen lässt, um weitere Informationen über den Schlüssel zu erhalten.
- **<hash>.0:** Die .0-Datei ist eine vertrauenswürdige Zertifikatsdatei, deren Inhalt mit der .CRT-Datei identisch ist. Ihr Name wird jedoch so gewählt, dass der Computer die Zertifikatsdatei in einem Verzeichnis, das viele verschiedene Zertifikate enthält, schnell findet. Der Name ist ein Hash (Prüfsumme) der Subjektinformationen des Zertifikats. Um den Hash-Dateinamen eines bestimmten Zertifikats zu bestimmen, zeigen Sie die <Schlüsselname>.CRT-Datei an. Die Datei enthält einen .INI-Dateiabschnitt [LDMS]. Das Hash=Wert-Paar gibt den <Hash>-Wert an.

Alle Schlüssel sind auf dem Core Server gespeichert unter \Programme\LANDesk\Shared Files\Keys. Der öffentliche <hash>.0 Schlüssel befindet sich auch im LDLOGON-Verzeichnis und muss dort standardmäßig abgelegt sein. <Schlüsselname> ist der Zertifikatsname, den Sie während des Setups für den Core Server bereitgestellt haben. Während des Setups ist es hilfreich, einen beschreibenden Schlüsselnamen anzugeben, z. B. den Namen des Core Servers (oder sogar dessen vollständig qualifizierten Namen). Beispiel: ldcore oder ldcore.org.com). Dies vereinfacht die Identifizierung des Zertifikats/des privaten Schlüssels in einer Umgebung mit mehreren Cores.

Sichern und Wiederherstellen von Dateien für Zertifikate / private Schlüssel auf Core Servern

Wenn Sie einen Core Server installieren, erstellt Setup ein neues Zertifikat. Auch wenn Sie über einen vorhandenen Core Server neu installieren, erstellt Setup dennoch ein neues Zertifikat. Wenn Sie Geräte installieren, die über ein Zertifikat verfügen, das nicht mit Ihrem neuen Core Server-Zertifikat übereinstimmt, kann der Core Server nicht mit diesen Geräten kommunizieren. Wenn Sie Ihren Core Server neu installieren müssen, haben Sie zwei Möglichkeiten:

1. Installieren Sie die Agenten manuell mit einer Konfiguration neu, die auf Ihrem neuen Core Server erstellt wurde. Sie können die Agenten nicht mit der Softwareverteilung aktualisieren, da Zertifikat und Schlüssel auf dem Core Server und den Geräten nicht übereinstimmen.

2. Legen Sie vor dem Neuinstallieren eines Core Servers eine Sicherungskopie des vorhandenen Zertifikats und der Schlüsseldateien an. Kopieren Sie die alten Schlüssel nach Abschluss der Installation auf die neue Core-Installation. Die neuen und alten Schlüssel können gleichzeitig vorhanden sein. Der Core verwendet automatisch den richtigen Schlüssel.

Cores können mehrere Dateien für Zertifikate/private Schlüssel enthalten. Sofern sich ein Client mit einem der Schlüssel auf einem Core authentifizieren kann, ist die Kommunikation mit diesem Core möglich.

Dieses Produkt wird mit einem Dienstprogramm geliefert, das die zweite Option, die weiter oben aufgeführt ist, ausführt. Das Core-Daten-Migrationsprogramm (CoreDataMigration.exe) wird im Ordner \Programme\LANDesk\ManagementSuite installiert. Es ist für das Erstellen von Sicherungskopien und Kopieren von Daten wie Schlüssel und Zertifikate beim Installieren eines neuen Cores zuständig.

So speichern Sie einen Satz Zertifikate/private Schlüssel und stellen ihn wieder her

1. Öffnen Sie auf dem Quell-Core Server den Ordner \Programme\LANDesk\Shared Files\Keys.
2. Kopieren Sie die Dateien <Schlüsselname>.key, <Schlüsselname>.crt und <hash>.0 des Quellservers auf eine Diskette oder an einen anderen sicheren Speicherort.
3. Kopieren Sie auf dem Ziel-Core Server die Dateien vom Quell-Core Server in denselben Ordner (\Programme\LANDesk\Shared Files\Keys). Die Schlüssel werden umgehend angewendet.

Warnung: Achten Sie sorgfältig auf die Sicherheit der privaten Schlüsseldatei. Vergewissern Sie sich, dass der private Schlüssel <Schlüsselname>.key nicht manipuliert werden kann. Übertragen Sie den Schlüssel nicht mithilfe eines ungeschützten Verfahrens, beispielsweise einer E-Mail-Nachricht oder einer öffentlichen Dateifreigabe. Der Core Server verwendet diese Datei zur Authentifizierung von Geräten, und jeder Core Server mit passender <Schlüsselname>.key-Datei kann Remote-Ausführungen und Dateiübertragungen auf einem verwalteten Gerät veranlassen.

Tipps zur Fehlerbehebung

Die folgenden Tipps für die Fehlerkorrektur beziehen sich auf Probleme, die am häufigsten im Zusammenhang mit der Konsole auftreten.

Ich kann den Core nicht aktivieren.
Wenn Sie einen Core installiert und dann die Gerätezeit geändert haben, können Sie den Core nicht aktivieren. Sie müssen das Produkt neu installieren, um den Core zu aktivieren.

Bei dem Versuch, den Core zu aktivieren, wurde ein Fehler angezeigt, in dem gemeldet wurde, dass die Core Server-Datenbank nicht gelesen werden konnte.
Stellen Sie sicher, dass der Core Server physikalisch mit dem Netzwerk verbunden ist und über eine gültige Internet-Verbindung verfügt. Wenn ein Kabel nicht eingesteckt oder die Internet-Verbindung des Core Servers ungültig ist, kann der Aktivierungsprozess nicht ausgeführt werden.

Ich kenne die URL zu den Konsolenseiten nicht.
Wenden Sie sich an die Person, die den Core Server installiert hat, wahrscheinlich ist dies der Netzwerkadministrator Ihres Unternehmens. Im Allgemeinen lautet die URL für Server Manager und System Manager http://*core server machine name*/ldsm. Die URL für Management Suite lautet http://*core server machine name*/remote.

Als welcher Benutzer bin ich angemeldet?
Sehen Sie über der Leiste unterhalb des Namens LANDeskSystem Manager im Abschnitt **Verbunden als** nach.

An welchem Gerät bin ich angemeldet?
Sehen Sie über der Leiste unterhalb des Namens LANDeskSystem Manager im Abschnitt **Verbunden mit** nach.

Nach dem Starten von System Manager erhalte ich sofort die Meldung, dass die Sitzung abgelaufen ist.
Wenn Sie System Manager aus dem Menü "Favoriten" oder "Lesezeichen" mit der Erweiterung "/frameset.aspx" am Ende der URL öffnen, wird das Produkt nicht ordnungsgemäß gestartet. Beheben Sie diesen Fehler, indem Sie diese Erweiterung aus Ihrer "Lesezeichen"- oder "Favoriten"-Verknüpfung entfernen oder die URL (ohne Erweiterung) direkt in das Browser-Fenster einfügen.

Ich sehe einige Verknüpfungen im linken Navigationsfenster nicht.
Der Grund hierfür ist, dass Ihr Netzwerkadministrator die rollenbasierte Administration oder die Option für Sicherheit auf Funktionsebene in LANDeskSystem Manager verwendet und Sie dadurch an der Ausführung bestimmter Tasks, für die Sie eigentlich Rechte besitzen, gehindert werden.

Der Scanner kann keine Verbindung mit dem Gerät herstellen.
Wenn der Scanner keine Verbindung mit dem Gerät herstellen kann, überprüfen Sie, ob das Verzeichnis der Webanwendung korrekt konfiguriert ist. Wenn Sie https verwenden, benötigen Sie ein gültiges Zertifikat. Stellen Sie sicher, dass Sie ein gültiges Zertifikat besitzen.

Ich halte dem Fehler "Berechtigung verweigert", wenn ich versuche, auf die Konsole zuzugreifen.
Um die Sicherheit auf Funktionsebene in Windows 2000 und 2003 verwenden zu können,

müssen Sie die anonyme Authentifizierung deaktivieren. Überprüfen Sie die Authentifizierungseinstellungen auf der Website und den Ordner..\LANDesk\ldsm unter der Website.

1. Klicken Sie auf dem Server, der die Webkonsole hostet, auf **Start | Verwaltung | Internet Information Services (IIS)-Manager**.
2. Klicken Sie im Kontextmenü der **Standard-Website** auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Directory Security** im Abschnitt **Anonymer Zugriff und Authentifizierungskontrolle** auf **Bearbeiten**. Deaktivieren Sie die Option **Anonymen Zugriff aktivieren** und aktivieren Sie das Kontrollkästchen **Integrierte Windows-Authentifizierung**.
4. Klicken Sie auf **OK**, um die Dialogfelder zu schließen.
5. Klicken Sie im Unterordner der Standard-Website .\LANDesk\ldsm auf **Eigenschaften**. Wiederholen Sie die Schritte 3 - 4.

Ich erhalte eine ungültige Sitzung beim Anzeigen der Konsole.
Es kann sein, dass die Browsersitzung abgelaufen ist. Verwenden Sie die Schaltfläche **Aktualisieren** Ihres Browsers, um eine neue Sitzung zu starten.

Beim Versuch, die Webkonsole zu starten, wird ein ASP.NET-Fehler angezeigt.
Wenn beim Versuch, auf die Webkonsole zuzugreifen, eine ASP.NET-Fehlermeldung angezeigt wird, sind möglicherweise ASP und die ASP-Verzeichnisberechtigungen nicht korrekt konfiguriert. Setzen Sie die ASP.NET-Konfiguration zurück, indem Sie folgenden Befehl ausführen:

```
ASPNET_REGIIS.EXE -i
```

Die Anzahl der Objekte pro Seite stimmt nicht mit der von mir angegebenen Zahl überein.
Die Einstellung, mit der Sie angeben, wie viele Objekte pro Seite angezeigt werden sollen, wird im Cookie-Verzeichnis des Browsers gespeichert und wird deaktiviert, wenn das Sitzungs-Timeout der Konsolensitzung abläuft.

Das Sitzungs-Timeout für die Konsole läuft zu häufig ab.
Sie können das standardmäßige Sitzungs-Timeout für die Webseiten der Konsole ändern. Der IIS-Standard liegt bei 20 Minuten Inaktivität, bevor eine Anmeldung abläuft. So ändern Sie das IIS-Sitzungstimeout:

1. Öffnen Sie auf dem Webserver den IIS Internetdienst-Manager.
2. Erweitern Sie die Standardwebsite.
3. Klicken Sie mit der rechten Maustaste auf den Ordner **LDSM** und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Virtuelles Verzeichnis** auf **Konfiguration**.
5. Klicken Sie auf die Registerkarte **Anwendungsoptionen** und ändern Sie das Sitzungs-Timeout in den gewünschten Wert.

Hinweis: LANDeskSystem Manager 8.70 ist ein sitzungsbasiertes Produkt. Deaktivieren Sie nicht den Sitzungsstatus.

Berichtsdiagramme werden nicht ordnungsgemäß angezeigt.
Damit die in vielen Berichten enthaltenen interaktiven Balken- und Tortendiagramme angezeigt werden, muss Macromedia Flash Player* installiert sein. Stellen Sie sicher, dass Flash installiert ist, und führen Sie dann den Bericht erneut aus.

Warum sehe ich zwei Instanzen desselben Geräts in meiner Datenbank?
Haben Sie ein Gerät aus der Core-Datenbank gelöscht und mit "UninstallWinClient.exe" erneut installiert?

UninstallWinClient.exe befindet sich in der LDMain-Freigabe, dem Hauptprogrammordner von ManagementSuite. Nur Administratoren haben Zugriff auf diese Freigabe. Dieses Programm deinstalliert LANDesk-Agenten auf jedem Gerät, auf dem es ausgeführt wird. Sie können es in jeden gewünschten Ordner verschieben oder zu einem Anmeldeskript hinzufügen. Es handelt sich dabei um eine Windows-Anwendung, die im Hintergrund ausgeführt wird, ohne eine Benutzeroberfläche einzublenden. Sie sehen möglicherweise zwei Instanzen des Geräts, das Sie gerade gelöscht haben, in der Datenbank. Eine dieser Instanzen enthält nur Protokolldaten, während die andere nach vorne gerichtete Daten enthält. Weitere Informationen zur UninstallWinClient.exe finden Sie im *Bereitstellungshandbuch*.

Wenn ich versuche, ein IPMI-Gerät erkennen zu lassen, wird es nicht im IPMI-Ordner auf der Seite "Nicht verwaltete Geräte" aufgeführt.
IPMI-Geräte müssen über einen konfigurierten BMC (Baseboard Management Controller) verfügen, damit sie als IPMI-Geräte erkannt werden und die IPMI-Funktionalität in vollem Umfang nutzen können. Wenn der BMC nicht konfiguriert ist, können Sie das Gerät als Computer erkennen lassen. Anschließend können Sie das Gerät zur Liste mit den verwalteten Geräten hinzufügen und das Dienstprogramm "Dienste konfigurieren" ausführen, um das BMC-Kennwort zu konfigurieren. Die IPMI-Funktionalität des Geräts wird dann von diesem Produkt erkannt.

Ich habe ein S.M.A.R.T.-Laufwerk auf einem Server hinzugefügt, jedoch wird die S.M.A.R.T.-Laufwerksüberwachung für diesen Server in der Inventarliste nicht angezeigt.
Die Hardwareüberwachung ist von der Funktionalität der auf dem Gerät installierten Hardware sowie von der korrekten Konfiguration der Hardware abhängig. Wenn z.B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden keine Überwachungsdaten bereitgestellt und auch keine resultierenden Alarme generiert.

Ein USB-Datenträgergerät wird erst in der Inventarliste angezeigt, nachdem ein Inventarscan ausgeführt wurde.
Wenn ein Datenträgergerät mit einem USB-Kabel an ein verwaltetes Gerät angeschlossen ist, wird es nicht sofort unter "Festplattenlaufwerke" im Inventar des Geräts aufgeführt. Es wird unter "Logische Laufwerke" aufgelistet, nachdem es mit dem Gerät verbunden wurde. Es wird erst unter "Festplattenlaufwerke" angezeigt, nachdem ein Inventarscan auf dem Gerät ausgeführt wurde.

Auf verwalteten Linux-Geräten muss ein USB-Datenträgergerät gemountet werden, damit es im Inventar aufgelistet wird. Wenn es gemountet wird, aber noch kein Inventarscan ausgeführt wurde, wird es unter "Logische Laufwerke" angezeigt; nach Ausführung des Inventarscans wird es auch unter "Festplattenlaufwerke" angezeigt. Wenn das Gerät getrennt wird, sollte es aus dem System deaktiviert (Dismounting) werden. Auf einigen Linux-Systemen, die einen älteren Kernel ausführen, verbleibt das Gerät u.U. in der Liste, selbst nachdem es getrennt und deaktiviert wurde. In diesem Fall muss das verwaltete Gerät neu gebootet werden, damit es aus der Inventarliste gelöscht wird.

Der Index der Webkonsolenhilfe ist beim Anzeigen leer.
Die HTML-Onlinehilfe der Webkonsole verfügt über eine Volltext-Suchfunktionen, die auf dem Indexdienst von Windows basiert. Normalerweise ist diese Funktion standardmäßig aktiviert.

Wenn Sie das Indizieren auf dem Webserver aktivieren müssen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Start | Programme | Verwaltung | Dienste**.
2. Doppelklicken Sie auf **Indexdienst** und klicken Sie auf **Start**.
3. Klicken Sie auf **OK**, um die Dialogfelder zu schließen.

Möglicherweise kann einige Zeit vergehen (u. U. mehrere Stunden), bis der Indexing Service einen Index für Ihren Server erstellt hat.